Cisco IoT Field Network Director リリース 3.2.x ユーザ ガイド

初版:2017 年 2 月

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、この参照により本書に組み込まれます。添付されていない場合には、代理店にご連絡ください。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

Cisco IoT Field Network Director の概要

この項では、Cisco IoT Field Network Director（Cisco IoT FND）の概要を示し、Cisco Internet of Things（IoT）ネットワーク ソリューション内で果たすその役割について説明します。次の内容について説明します。

Cisco IoT Connected Grid ネットワーク

ここでは、次についての概要を示します。

Cisco IoT Field Network Director（IoT FND）は、スマート グリッド アプリケーションなどの IoT アプリケーション用の、マルチサービス ネットワークやセキュリティ インフラストラクチャを管理するソフトウェア プラットフォームです。このスマート グリッド アプリケーションには、Advanced Metering Infrastructure（AMI）、Distribution Automation（DA）、分散インテリジェンス、および変電所オートメーションなどが含まれます。IoT FND は、拡張可能なアーキテクチャを備えた、スケーラブルで、高度にセキュアで、モジュラ形式のオープン プラットフォームです。IoT FND は、マルチベンダーでマルチサービスの通信ネットワーク管理プラットフォームであり、電力グリッド デバイスのオープン エコシステムへのネットワーク接続を可能にします。

IoT FND は、ネットワーク管理機能とアプリケーション（分散管理システム（DMS）、停止管理システム（OMS）、およびメーター データ管理（MDM）など）とを明確に分離できる、層化システム アーキテクチャ上に構築されます。ネットワーク管理とアプリケーションとのこの明確な分離は、公益事業企業が（たとえば AMI を使用して）スマート グリッド プロジェクトを徐々に展開するのに役立ちます。さらに、さまざまな公益事業の業務で、共有のマルチサービス ネットワーク インフラストラクチャと共通のネットワーク管理システムを使用した分散オートメーションを拡大していくのに役立ちます。

機能

- 地理情報システム（GIS）マップ ベースの仮想化、モニタリング、トラブルシューティング、およびアラーム通知
- フィールドエリア ルータ（FAR）とスマート メーター エンドポイントのグループ ベース設定管理
- OS 互換（ゲスト OS）、およびアプリケーション管理の提供
- カスタマイズ可能なしきい値ベースのアラーム処理とイベント生成用のルール エンジン インフラストラクチャ
- ユーティリティ ヘッドエンドと運用システムとの透過的な統合用の North Bound API
- 高可用性/ディザスタ リカバリ

Cisco IoT FND は、強力な地理情報システム（GIS）による視覚化およびモニタリング機能を備えています。ユーティリティ オペレータは、ブラウザベースのインターフェイスにより、6LoWPAN（IPv6 over Low-power Wireless Personal Area Networks）を使用する、Cisco IoT Connected Grid Field Area Network（FAN）ソリューションでデバイスを管理およびモニタできます。FAN には、次のデバイスが含まれます。

- Cisco 1000 Series Connected Grid ルータ（CGR）。これはポールトップまたは DIN レールマウント ルータとも呼ばれます。これらのデバイスは、このマニュアルでは FAR と表記されており、[Field Devices] ページでモデル別（たとえば、CGR1000、CGR1120、CGR1240）に示されています。使用可能な CGR モジュールは、3G、4G LTE、およびメッシュ接続（WPAN）を提供します。CGR1000 は Itron OpenWay RIVA CAM モジュールもサポートし、これは Itron OpenWay RIVA 電気およびガス水道デバイスへの接続を提供します。

- Cisco 800 Series Integrated Services ルータ（ISR 800）は、ほとんどのネットワークでエッジ ルータまたはゲートウェイとして使用されており、エンド デバイス（エネルギー供給自動化デバイス、ATM などの他の特定業種向けデバイス、およびタクシーやトラックなどのモバイル配備）への WAN 接続（セルラー、イーサネット経由のサテライト、および WiFi）を提供します。これらのデバイスは、このマニュアルでは FAR と表記されており、[Field Devices] ページで製品 ID 別（たとえば、C800 や C819）に示されています。IoT FND を使用して、強化された次の Cisco 819H ISR を管理できます。

  - C819HG-4G-V-K9
  - C819HG-4G-A-K9
  - C819HG-U-K9
  - C819HGW-S-A-K9
  - C819H-K9

  IoT FND は、強化されていない次の Cisco 819 ISR も管理します。

  - C819G-B-K9
  - C819G-U-K9
  - C819G-4G-V-K9
  - C819G-7-K9

- Cisco 800 シリーズ サービス統合型ルータ（IR800）は、コンパクトで耐久性の高い Cisco IOS ソフトウェア ルータです。これらは、統合 4G LTE ワイヤレス WAN（IR809 と IR829 の両方のモデル）と、ワイヤレス LAN 機能（IR829 のみ）のサポートを提供します。これらのデバイスは、このマニュアルでは FAR と表記されており、[Field Devices] ページで製品 ID 別（たとえば、IR800）に示されています。IoT FND を使用して、次の IR800 モデルを管理できます。

  - IR809
  - IR829

- Cisco Interface Module for Long Range Wide Area Network（LoRAWAN）は、産業用ルータ Cisco IR809 および IR829 の拡張モジュールであり、屋外配備用のキャリア グレード ゲートウェイとして機能します。このモジュールは、幅広い Internet of Things（IoT）ユース ケースに対応する、ライセンス不要の低電力広域（LPWA）ワイヤレス接続を提供します。このユース ケースには、アセット トラッキング、水道やガスの検針、街路灯、スマート パーキング/ビルディング/農業/環境モニタリングなどがあります。2 つのモデルがサポートされており、それらはそのバンド サポート（863 ～ 870 MHz ISM または 902 ～ 928 MHz ISM）により区別されます。

- Cisco 500 シリーズ無線パーソナル エリア ネットワーク（WPAN）産業用ルータ（IR500）は、RF メッシュ接続を、IPv4 およびシリアル Internet of Things（IoT）デバイス（たとえば、リクローザ制御、キャップ バンク制御、電圧レギュレータ制御、および他のリモート端末ユニット）に提供します。

  （注）CGR、C800、IR800、IR500、および他のタイプのメッシュ エンドポイント デバイスは、ネットワーク上に共存できますが、同じデバイス グループに入れることはできません（デバイス グループの作成およびメッシュ エンドポイント ファームウェア イメージの使用を参照）。また同じファームウェア管理グループに入れることもできません（ファームウェア グループの設定）。

- Cisco 800 シリーズ アクセス ポイントは、IR800 および C800 と統合されています。これらのデバイスは、このマニュアルでは FAR と表記されており、製品 ID 別（たとえば、AP800）に示されています。IoT FND を使用して、次の AP800 モデルを管理できます。
  - C800 に組み込まれた AP802
  - IR829 に組み込まれた AP803
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ（ASR）および Cisco ISR 3900 シリーズ サービス統合型ルータ（ISR）。このマニュアルでは*ヘッドエンド ルータ*または HER と表記しています。
- Cisco IPv6 RF（無線周波数）、PLC（電力線通信）、およびデュアル PHY（RF および PLC）メッシュ エンドポイント（スマート メーターおよび Range Extender）。

(注) このマニュアルでは、*メッシュ エンドポイント*（ME）は、Cisco Range Extender および Cisco 互換スマート メーターのことを指します。

IoT FND は通常、ユーティリティ コントロール センターに、他のユーティリティ ヘッドエンド運用システム（AMI ヘッド エンド、分散管理システム、または停止管理システム）とともに置かれます。IoT FND は、オープン システム相互接続（OSI）モデルで定義されている、企業クラスの FCAPS（障害、設定、アカウンティング、パフォーマンス、およびセキュリティ）機能を特色としています。

Cisco IoT FND North Bound Application Programmable Interface（NB API）により、DMS、OMS、MDM などのさまざまなユーティリティ アプリケーションは、共有マルチサーバ通信ネットワーク インフラストラクチャから、分散グリッド情報、停止情報、および測定データについての適切なサービス固有データを取り出すことができます。Cisco IoT FND North Bound API の詳細は、ご使用の IoT FND インストール バージョンの『*Cisco IoT FND NMS North Bound API Programming Guide*』を参照してください。

NB API は、HTTPS を使用してイベントを送信できます。NB API クライアントは、イベント送信のための有効な URL HTTPS を提供することで、IoT FND をサブスクライブする必要があります。IoT FND は、NB API クライアント（イベント コンシューマ）によりパブリッシュされたすべての SSL およびハンドシェイク証明書を受け入れ、同時にセキュア接続を確立します。

Cisco IoT FND の機能

- **設定管理**：Cisco IoT FND により、多数の Cisco CGR、Cisco C800、Cisco ISR、Cisco IR、Cisco ASR、および ME の設定を容易に実行できるようになります。Cisco IoT FND は、デバイスを設定グループ内に配置し、設定テンプレートで設定値を編集し、その設定をグループ内のすべてのデバイスにプッシュすることで、デバイスを一括設定します。
- **デバイスとイベントのモニタリング**：Cisco IoT FND は、デバイスが生成した詳細情報を読みやすい表形式ビューで表示し、これによりユーザはネットワークのエラーをモニタできます。Cisco IoT FND は、ルータやスマート メーターなどの FAN デバイスを、統合された地理情報システム（GIS）マップベースで視覚化します。ルータへのアクセスに必要な証明書を含む CGR 固有のワーク オーダーを作成するには、IoT FND を使用します。
- **ファームウェア管理**：Cisco IoT FND は、Cisco CGR、Cisco C800、Cisco ISR、Cisco IR、および ME ファームウェア イメージのリポジトリとして機能します。Cisco IoT FND を使用して、デバイスのグループで実行するファームウェアをアップグレードするには、ファームウェア イメージ ファイルを Cisco IoT FND サーバに読み込ませ、次にイメージをグループ内のデバイスに読み込ませます。アップロードしたら、IoT FND を使用してファームウェア イメージをデバイスに直接インストールします。リリース 3.0.1-36 以降では、メッシュ エンドポイントの [Firmware Upgrade] ページのサブネット リスト ビューで、PAN 識別子（PAN ID）およびグループによりサブネットをフィルタリングして表示できます（詳細にはグループ内のノードの数、ルータからのホップ数、操作ステータスなどが含まれます）。サブネット進捗ヒストグラムも追加されています。
- **OS 移行**：Cisco CGR 1000 の場合、IoT FND により、CG-OS を実行する CGR を IOS に移行できます。
- **ゼロ タッチ導入**：この使いやすい機能は、X.509 証明書とプロビジョニング情報を、Connected Grid ネットワーク内のセキュアな接続を介して自動的に登録して配布します。
- **トンネル プロビジョニング**：Cisco ASR、Cisco CGR、C800、Cisco ISR、および Cisco IR の間で交換されるデータを保護し、Cisco CGR への無許可アクセスを防止して、デバイス間でのセキュア通信を提供します。Cisco IoT FND では、CLI コマンドを実行して、Cisco CGR、C800、Cisco ISR、Cisco IR、および Cisco ASR の間にセキュア トンネルをプロビジョニングできます。グループを使用してトンネル プロビジョニングを一括設定するには、IoT FND を使用します。

- **IPv6 RPL ツリー ポーリング**：IPv6 Routing Protocol for Low-power and Lossy Networks（RPL）は、そのネイバーを検出し、ICMPv6 メッセージ交換を使用してルートを確立します。RPL は、ルーティング ツリーのルートである CGR に対する ME の相対位置に基づいて、ルートを管理します。RPL ツリー ポーリングは、メッシュ ノードと CGR 定期更新により使用可能になります。RPL ツリーはメッシュ トポロジを表しますが、これはトラブルシューティングに役立てることができます。たとえば、RPL ツリーから受け取ったホップ カウント情報により、ファームウェア ダウンロード プロセスのユニキャストまたはマルチキャストの使用を判別できます。IoT FND は、RPL ツリーの定期的に更新されるスナップショットを保持します。
- **動的マルチポイント VPN および FlexVPN**：Cisco C800 デバイスと Cisco IR800 デバイスの場合、DMVPN と FlexVPN は、トンネル プロビジョニング時にデバイス固有のトンネル設定を HER に適用するために IoT FND を必要としません。HER トンネル プロビジョニングは、サイト間 VPN トンネルにのみ必要です。
- **組み込みアクセス ポイント（AP）管理**：IoT FND は、C819 および IR829 ルータ上の組み込み AP を管理します。
- **デュアル PHY サポート**：IoT FND は、デュアル PHY（RF および PLC）トラフィックをサポートするデバイスと通信できます。IoT FND は、デュアル PHY を実行する CGR を識別し、マスターとスレーブへの設定を有効化し、マスターからメトリックを収集します。IoT FND はさらに、デュアル PHY CGR のセキュリティ キーを管理します。メッシュ側で、IoT FND は固有のハードウェア ID を使用してデュアル PHY ノードを識別し、設定のプッシュとファームウェアの更新を可能にし、RF や PLC トラフィック率を含むメトリックを収集します。
- **ゲスト OS（GOS）サポート**：ゲスト OS をサポートする Cisco IOS CGR 1000 および IR800 デバイスの場合、IoT FND はサポート対象オペレーティング システム上で実行するアプリケーションの管理を、承認取得済みユーザに許可します。IoT FND はアプリケーション導入のすべてのフェーズをサポートし、アプリケーションのステータスと、デバイス上で実行する Hypervisor のバージョンを表示します。
- **デバイス ロケーションのトラッキング**：CGR 1000、C800、および IR800 デバイスの場合、IoT FND はリアルタイム ロケーションとデバイス ロケーションの履歴を表示します。この機能は、GPS 機能を有効にすることが必要です。
- **ソフトウェア セキュリティ モジュール（SSM）**：これはハードウェア セキュリティ モジュール（HSM）の低コスト代替製品であり、メーターや IR500 デバイスに送信される CSMP メッセージの署名に使用されます。
- **カスタマー証明書**：Cisco IoT FND は、ユーザが独自の CA と ECC ベースの証明書を使用してスマート メーター メッセージに署名することを許可します。
- **診断およびトラブルシューティング**：IoT FND ルール エンジン インフラストラクチャは、トリアージ ベース トラブルシューティングによる効率的なモニタリングを行うことができます。デバイスのトラブルシューティングでは、オンデマンドのデバイス パス トレースおよび ping を、すべての CGR、Cisco C800、Range Extender、またはメーター（メッシュ エンドポイント）に対して実行します。
- **高可用性**：中断のないネットワーク管理とモニタリングを確実にするために、Cisco IoT FND ソリューションは高可用性（HA）構成で展開できます。ロード バランシングが行われる IoT FND サーバとプライマリおよびスタンバイ IoT FND データベースを使用することで、Cisco IoT FND は、システムのヘルス（クラスタ内の接続やサーバ リソースの使用状況を含む）を常時モニタします。サーバ クラスタのメンバーまたはデータベースが使用できなくなったかまたはトンネルに障害が発生すると、別のメンバーまたはデータベースがシームレスに引き継ぎます。さらに、Cisco CGR と複数の Cisco ASR の間に冗長トンネルを構成することで、IoT FND の信頼性を向上させることができます。
- **停電通知**：Connected Grid Endpoint（CGE）は、停電についてのタイムリーで効率的なレポート作成をサポートする、停電通知サービスを実装します。停電時に、CGE は、エネルギーを節約するために必要な機能を実行し、ネイバー ノードに停電を通知します。FAR は IoT FND への停電通知を中継し、停電に関する情報を関連付けるプッシュ通知を顧客向けに発行します。
- **メッシュ アップグレード サポート**：Cisco CGR および CGE などのフィールド デバイス（たとえば、AMI メーター エンドポイント）のソフトウェアおよびファームウェアをワイヤレスでアップグレードできます。
- **監査ロギング**：監査、法規制の遵守、および SEIM（セキュリティ イベントおよびインシデント管理）の統合などのユーザ アクティビティのアクセス情報をログに記録します。これにより管理は簡素化され、モニタ、レポート、およびトラブルシューティングの各機能の統合によりコンプライアンスが強化されます。
- **North Bound API**：停止管理システム（OMS）、メーター データ管理（MDM）、トラブル チケット システム、およびマネージャ オブ マネージャズなどの既存のユーティリティ アプリケーションを簡単に統合できます。
- **デバイス マネージャのワーク オーダー**：資格を持つ現場技術者は、ワーク オーダーにリモートにアクセスしてそれを更新できます。

- **ロールベース アクセス コントロール**：AMI ネットワーク デバイス用にエンタープライズ セキュリティ ポリシーとロールベース アクセス コントロールを統合します。
- **イベントおよび問題の管理**：障害イベントの収集、フィルタリング、および通信ネットワーク モニタリングの相関を行います。IoT FND は、しきい値ベースのルール処理、カスタム アラート生成、およびアラーム イベント処理のための多様な障害イベント メカニズムをサポートします。ユーティリティ ネットワーク内のさまざまなエンドポイントについて、障害は色分けされた GIS マップ ビューで表示されます。これにより、停止管理システムなどのさまざまなユーティリティ アプリケーションに対する、オペレーターレベルのカスタムでの、障害イベントの生成、処理、および転送が可能になります。自動問題追跡は、収集されるイベントに基づいて実行されます。

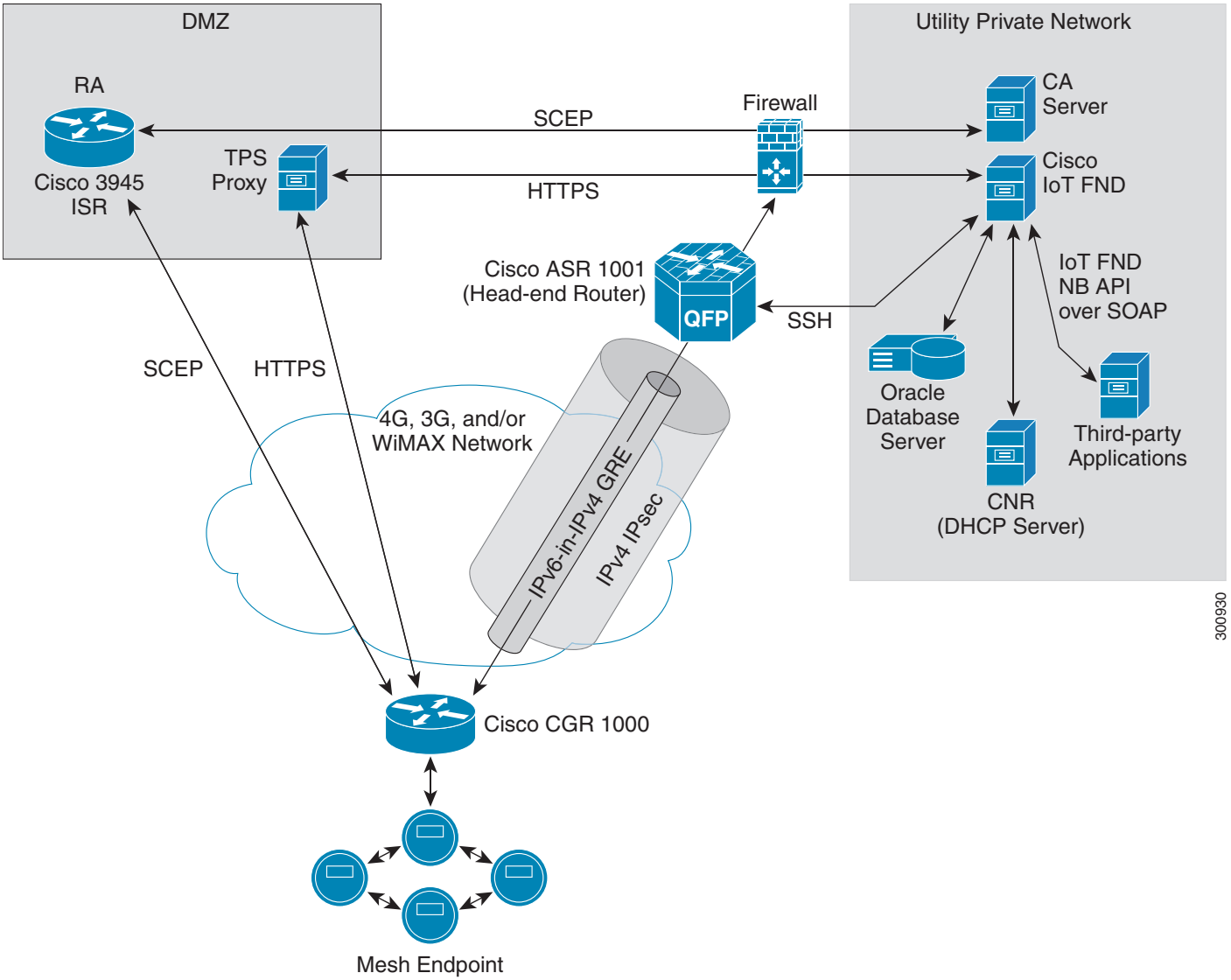
IoT FND のアーキテクチャ

図 1 は、標準的な公益事業企業の、内部でゼロ タッチ展開を使用している Cisco CGR Connected Grid ネットワーク上で運用されている、システム パスと通信パスの概略図です。

Cisco IOS CGR には、FlexVPN を使用したトンネル構成を推奨します。FlexVPN は、これらすべての機能を（IPsec により保護された）1 つの GRE トンネルに結合します。

Cisco C800 および IR800 には、動的マルチポイント VPN（DMVPN）または FlexVPN を使用することを推奨します。

図 1　　ゼロ タッチ展開アーキテクチャ



この例では、ファイアウォールにより、公益事業企業のパブリック ネットワーク（DMZ）とそのプライベート ネットワークの項目が区分されています。

公益事業企業のプライベート ネットワークには、ファイアウォールの背後に置くことができるシステム（Cisco IoT FND、Oracle データベース サーバ、Cisco IoT FND North Bound API、DHCP サーバ、認証局（CA）など）が示されています。Cisco IoT FND トンネル プロビジョニング サーバ プロキシ（TPS プロキシ）や登録局（RA）も DMZ 内に置くことができます。

Cisco CGR をインストールして電源をオンにすると、ネットワーク内でアクティブになり、SCEP（Simple Certificate Enrollment Protocol）を使用してその証明書を RA に登録します。RA（図 1 の Cisco 3945 ISR）は、CA プロキシとして機能し、CA から Cisco CGR の証明書を取得します。Cisco CGR は、トンネル プロビジョニング要求を HTTPS を介して TPS プロキシに送信し、要求はそこから IoT FND に転送されます。

Cisco IoT FND は、Cisco CGR とヘッドエンド ルータ（図 1 の Cisco ASR 1001）との間のトンネルを設定するために必要なすべての情報のコレクションを管理します。CG-OS CGR インストール システムの場合は、外部は IPv4 を介した IPsec トンネルで、その内部は IPv6-in-IPv4 GRE トンネルであるネットワーク構成を推奨します。ME からのすべてのトラフィックは IPv6 を介して送信されます。GRE トンネルは、データ センターにアクセスするために IPv6 トラフィックのパスを提供します。外部 IPsec トンネルにより、そのトラフィックは保護されます。トンネルをアクティブにすると、Cisco CGR（設定後）は、公益事業企業の仮想プライベート ネットワーク（VPN）のようなネットワークに接続します。

IoT FND ソリューションのメイン コンポーネント

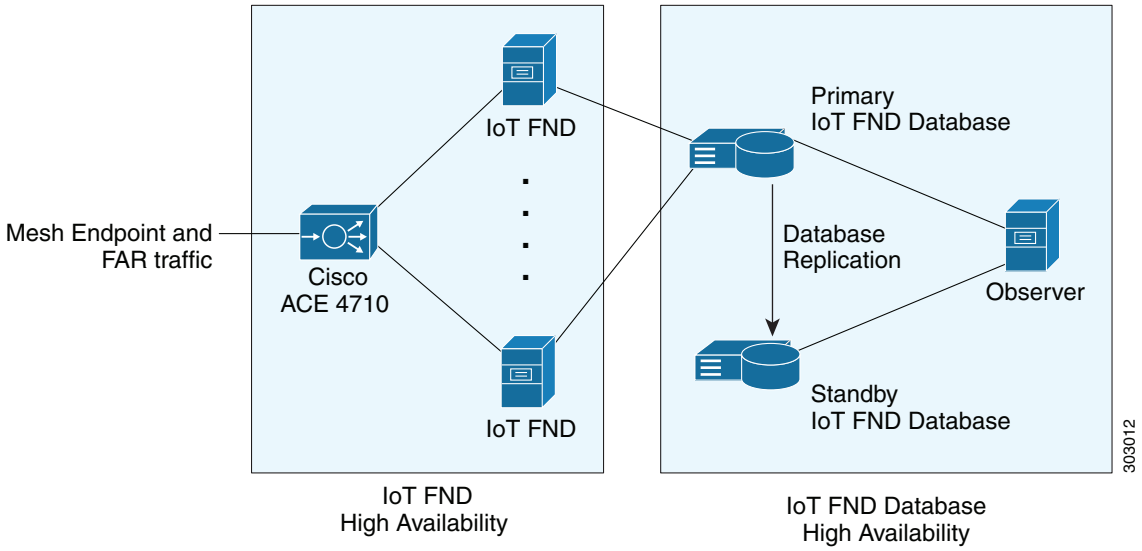
コンポーネント	説明
IoT FND アプリケーション サーバ	IoT FND 導入システムの中心機能です。これは RHEL サーバ上で稼働し、これによって管理者は、ブラウザベースのグラフィカル ユーザ インターフェイスを使用して、IoT FND 導入システムのさまざまな面を制御できます。 IoT FND HA 導入システムには、ロード バランサに接続された 2 つ以上の IoT FND サーバが含まれています。
NMS データベース	この Oracle データベースには、IoT FND ソリューションによって管理されるすべての情報が保存されます。これには ME から受信したすべてのメトリックや、ファームウェア イメージ、設定テンプレート、ログ、イベント情報などのすべてのデバイス プロパティが含まれます。
ソフトウェア セキュリティ モジュール(SSM)	これはハードウェア セキュリティ モジュール(HSM)の低コスト代替製品であり、メーターや IR500 デバイスに送信される CSMP メッセージの署名に使用されます。
TPS プロキシ	現場での最初の起動時に FAR が IoT FND と通信できるようにします。IoT FND が FAR と ASR との間のトンネルをプロビジョニングしたら、FAR は IoT FND と直接通信します。
ロード バランサ	(任意)IoT FND は図 1 の Cisco ACE 4710 を使用して HA を備えます。ロード バランサは、ソリューションのサーバ クラスタ内にある IoT FND サーバ間でトラフィックを分散させます。

高可用性とトンネル冗長性

図 1 で示す例は、1 つのデータベースがあり、トンネル冗長性はない、単一サーバ導入システムです。ただし、Cisco IoT FND HA サポートを利用して、Cisco ACE 4710 ロード バランサに接続されている Cisco IoT FND サーバのクラスタを導入できます(図 2 を参照)。ロード バランサは、ラウンドロビン方法で要求をサーバに送信します。サーバに障害が発生すると、ロード バランサは、クラスタ内の他のサーバに送信することで要求を処理し続けます。

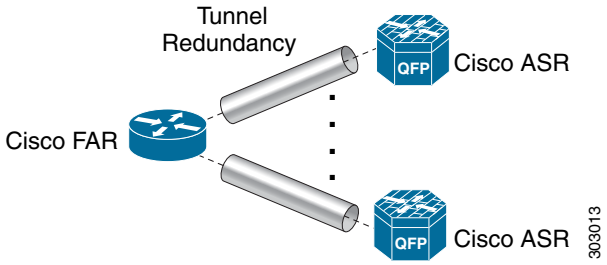
最小限のデータ ロスでシステム内に高可用な別の層を備えるには、スタンバイ Cisco IoT FND データベースを導入することもできます。

図 2　　IoT FND サーバおよびデータベース HA



トンネル冗長性を備えるために、IoT FND では CGR を複数の ASR に接続するための複数のトンネルを作成できます（図 3 を参照）。

図 3　　IoT FND トンネルの冗長性



HA の詳細については、データベース ハイ アベイラビリティを参照してください。

メッシュ エンドポイント

Cisco Field Area Network（FAN）ソリューションは、初めてのマルチサービス通信インフラストラクチャを、公益事業者のフィールド エリア ネットワークに導入します。これは、AMI や DA、および共通ネットワーク プラットフォームの保護と制御のためのアプリケーションを提供します。

高機能メーターを導入したら、続いては公益事業企業のニーズに適正なソリューションで応えるように設計された構造化プロセスを導入することになります。このプロセスは、計測、IT、操作、およびエンジニアリングの間での調整を必要とするいくつかのフェーズを経て進められます。ほとんどの公益事業企業にとって最初のフェーズは、目標を特定することであり、それにデータ分析のニーズやビジネス プロセスが続きます。ビジネス ケースの評価が完了し、テクノロジが選択されたら、システムの実装と検証のプロセスを実行します。

公益事業企業が過去のビジネス ケースを現在のシステム実装に移そうとすると、予測できない複雑さにより導入が遅延する場合があります。プラグ アンド プレイ システムの真価は、高機能計測をより短時間で実現できるという利点により、コストを節約し、投資回収率を向上させることにあります。

真のプラグ アンド プレイ RF または PLC メッシュ ネットワーク システムを実現する機能には、次のものがあります。

- **自己初期化エンドポイント**：CGR は、メーターやインフラストラクチャ展開をプログラミングなしに検出する高度な自己検出により、通信のための最善のパスを自動的に確立します。
- **拡張性**：このタイプのネットワークにより、Cisco IoT FND インストール システムは、最大で 1000 万のメーター/エンドポイントに対応できる、ポケット化された導入システムを実現できます。キャパシティが大きいため、対象の AMI カバレッジ エリアのさまざまな箇所で迅速な複数チームでの導入を実行でき、インフラストラクチャや通信のコストを節約できます。

真のメッシュ ネットワークでは、測定デバイスやレンジ エクステンダ デバイスは相互に通信し、独自の最良リンクを決定して、メッシュ ローカル エリア ネットワーク（RFLAN）または PLC LAN を形成します。これらの ME デバイスはネットワークを形成し、動的自動ルーティング機能を持つようになります。この機能により、専用リピータ インフラストラクチャや中間層の（エンドポイントとコレクタの間の）ラジオ リレー ネットワークを省くことができます。結果として、専用ネットワーク インフラストラクチャと、強力で柔軟性が高い固定ネットワーク通信機能をかなり削減することができます。

Range Extender は、公益事業企業により、メッシュのカバレッジを強化し、冗長性を備えるためにインストールされます。さらに、建造物が通常のメッシュ信号伝搬を妨げる密集した都市部、地理的にメーター密度が低く人口密度が低い地域、高周波が問題となる地域などの困難な環境設定でネットワーク信頼性を補うためにもインストールされます。Range Extender は、インストールまたは停止リカバリ後のメッシュを自動的に検出して接続し、代替メッシュ パスを提供します。

通常の導入シナリオでは、これらの ME は、導入されたその日から安定した RFLAN または PLC LAN ネットワークを形成します。コレクタがインストールされたら、導入エリア全体に ME を配置することは、メーターの交換と同じほど簡単になります。ME は自動的にネットワークを形成してレポートを開始します。

メッシュ エンドポイントは情報を送受信します。双方向メッシュ システムにより、リモート ファームウェア アップグレード、使用期間のシステム設定の変更やコマンド実行、需要リセット、および停止復元通知などが行えるようになります。物理的に「メーターに触る」必要がないことには大きな価値があります。特定のクライアントのニーズを満たすために、使用時間（TOU）スケジュールの変更

と間隔データ取得の変更が必要である、高度デマンド応答測定ドメインに入る場合は特にそのように言えます。これらのコマンドは、グループまたは特定の ME に送信できます。メーター コマンドは、スケジュール指定、プロアクティブ、オンデマンド、またはネットワーク全体へのブロードキャストのいずれかで実行できます。

データセンター/ネットワーク オペレーション センター(NOC)とコレクタとの間の通信は、広く入手可能でコスト効率の高い、市販の TCP/IP ベース パブリック ワイド エリア ネットワーク(WAN)または公益事業企業が所有する WAN のいずれかを利用して実現されます。現在利用できる柔軟でオープン標準のパブリック WAN アーキテクチャにより、将来的にも継続的にコスト削減が可能な環境を構成できます。資産の存続期間全体にわたって 1 タイプの接続性に拘束されることがないため、将来のオプションに対応することもできます。AMI システムで専門性が非常に高い WAN システムを使用しないのであれば、それが最善です。

導入が完了すると、システムはスケジュール設定された時間ごと(およびサブ時間ごと)のデータを送信して、請求書読み取り、高度デマンド応答イニシアチブ、負荷リサーチ、電源品質、および変圧器資産モニタリングなどのユーティリティ アプリケーションをサポートできます。

アクセスのしやすさと信頼できるオンデマンド機能により、ユーティリティはグリッド診断と負荷リサーチを、システム全体または選択したメーターのグループに対して実行できます。他の標準機能は、停止管理、改ざん検出、およびシステム パフォーマンス モニタリングをサポートします。

グリッド セキュリティ

次世代エネルギー ネットワークの要件を満たすように設計された Cisco グリッド セキュリティ ソリューションは、シスコのサイバーセキュリティおよび物理セキュリティ関連の製品、テクノロジ、サービス、パートナーの広範なポートフォリオを活用します。これにより公益事業企業は運用コストを削減しながら、重要なエネルギー インフラストラクチャのサイバーセキュリティと物理セキュリティを向上させることができます。

Cisco グリッド セキュリティ ソリューションは、次のものを提供します。

- **アイデンティティの管理およびアクセス制御**:ユーザ認証とアクセス制御を使用したユーティリティ機能、資産、およびデータの保護は、グリッド運用のためにカスタマイズ構築されます。
- **スレッド防御**:脅威を検出、回避、軽減するために、ファイアウォール、VPN、侵入防御、およびコンテンツ セキュリティ サービスと統合する階層型防御を構築します。
- **データセンター セキュリティ**:ネットワーク、コンピューティング、およびストレージの各ソリューションを、単一の安全なリソース共有プールに変換します。これによりアプリケーションとデータの整合性の保護、公益事業会社内のビジネス プロセスとアプリケーション間の通信の保護、および再生可能エネルギーのプロバイダなどの外部リソースへの接続の保護が実現します。
- **ユーティリティ コンプライアンス**:リスク管理を向上させ、アセスメント、設計、導入サービスにおいて NERC-CIP などの法規制要件を満たします。
- **セキュリティ モニタリングおよび管理**:情報セキュリティの脅威の特定、対処、および反撃を行い、サイバー イベントの継続的なモニタリングを通じてコンプライアンスを維持します。

関連ソフトウェア

次のソフトウェア パッケージは、Cisco Internet of Things(IoT)ネットワーク ソリューションの導入と管理を支援します。

Cisco IoT Device Manager

Cisco IoT Device Manager(Device Manager または IoT-DM)は、現場技術者が Cisco CGR をリモートに管理するために使用する、Windows ベースのアプリケーションです。いくつかのアクティビティでは、IoT DM は情報を IoT FND から取得します。

シスコ インダストリアル オペレーション キット

Cisco インダストリアル オペレーション キット(IOK)は、Cisco IoT ネットワーク ソリューション用に、管理、ネットワーク、および IOK セキュリティ関連ヘッドエンド ネットワーク サービスのための複数の仮想アプライアンスを組み込んでいます。詳細については、シスコの営業担当者にお問い合わせください。

このマニュアルの使い方

この項には、情報をすばやく見つけることができる次のトピックがあります。

共通タスク

表 1 は、FAR と ME の両方に対してユーザが実行するタスクをリストしています。タスクを実行できるかどうかは、ロールベースで割り当てられます。ユーザ ロールの詳細については、システム定義ユーザー ロールを参照してください。

表 1　　共通タスク

タスク	使用目的
デバイス表示タスク	
デバイスの表示	ルータの各ビューの使用、[Default] ビューでのエンドポイントの表示
詳細なデバイス情報の表示	デバイスの詳細情報の表示
デバイス分類タスク	
ラベルの追加	ラベルの一括追加
ラベルの削除	ラベルの一括削除
検索およびデバイス フィルタリング タスク	
フィルタの使用	フィルタを使用したデバイス表示の制御
診断およびトラブルシューティング タスク	
ping	デバイスの ping
traceroute	デバイスへのルートのトレース
ログのダウンロード	ログのダウンロード
タスクのモニタリング	
イベントの表示および検索	イベントのモニタリング
問題の表示および検索	モニタリングの問題、[Issues] ステータス バーでのデバイス重大度ステータスの表示
トンネル ステータスの表示	トンネル ステータスのモニタリング
一般的な作業	
パスワードの変更	パスワードのリセット
タイム ゾーンを設定する	タイム ゾーンの設定
ユーザ プリファレンスの設定	ユーザ プリファレンスの設定

CGR タスク

表 2 は、CGR タスクをリストしています。ユーザ ロールの詳細については、システム定義ユーザー ロールを参照してください。

表 2　　CGR タスク

タスク	使用目的
ルータ設定タスク グループ	
設定グループへの CGR の追加	デバイス グループの作成
構成グループの削除	デバイス グループの削除
設定グループ内のデバイスのリスト	設定グループ内のデバイスのリスト表示
グループへのデバイスの割り当て	IoT FND への FAR の追加 IoT FND への HER の追加 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
設定グループの名前の変更	デバイス設定グループの名前変更
ルータ設定タスク	
デバイス設定プロパティの変更	デバイス設定プロパティの変更
設定テンプレートの編集	ROUTER 設定テンプレートの編集 AP 設定テンプレートの編集
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
CG-OS から IOS への移行	OS の移行
アプリケーションの管理	GOS アプリケーションの管理
トンネル プロビジョニング タスク	
トンネル プロビジョニングの設定	トンネル プロビジョニングの設定
トンネル プロビジョニング テンプレートの編集	トンネル プロビジョニング テンプレートの設定
トンネルの再プロビジョニング	トンネル再プロビジョニング 出荷時再プロビジョニング
ファームウェア管理のタスク	
ファームウェア グループへのデバイスの割り当て	ファームウェア グループへのデバイスの割り当て
ファームウェア グループへのイメージのアップロード	FAR グループへのファームウェア イメージのアップロード
ワーク オーダー タスク	
ワーク オーダーの作成	ワーク オーダーの作成

メッシュ エンドポイント タスク

表 3 は、ME タスクをリストしています。ユーザ ロールの詳細については、システム定義ユーザー ロールを参照してください。

表 3　　メッシュ エンドポイント タスク

タスク	使用目的
ME 設定グループ タスク	
メッシュ エンドポイント設定グループの追加	デバイス グループの作成
メッシュ エンドポイント設定グループの削除	デバイス グループの削除
メッシュ エンドポイント設定グループの名前の変更	デバイス設定グループの名前変更
設定グループへのメッシュ エンドポイント デバイスの割り当て	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	設定グループ内のデバイスのリスト表示
ME 設定タスク	
メッシュ エンドポイント設定プロパティの変更	デバイス設定プロパティの変更
メッシュ エンドポイント設定テンプレートの編集	ENDPOINT 設定テンプレートの編集
メッシュ エンドポイントへの設定のプッシュ	メッシュ エンドポイントへの設定のプッシュ
メッシュエンドポイント ファームウェア グループの追加	デバイス グループの作成
ファームウェア グループへのデバイスの割り当て	別のグループへのデバイスの移動
ファームウェア グループへのイメージのアップロード	メッシュ エンドポイント グループへのファームウェア イメージのアップロード

管理タスク

表 4 は、管理タスクをリストしています。

表 4　　管理タスク

タスク	使用目的
システム管理タスク	
パスワード ポリシーの設定	パスワード ポリシーの管理
ロールの定義	ロールの管理
ユーザ アカウントの管理	ユーザの管理
アクセス管理タスク	
アクティブ セッションの管理	アクティブ セッションの管理
監査証跡の表示	監査証跡の表示
証明書を管理する	証明書の管理
データ保存の設定	データ保存の設定
ライセンスの管理	ライセンスの管理
ロギングの管理	ログの管理

表 4　　管理タスク（続き）

タスク	使用目的
サーバ設定値の設定	サーバ設定値の設定
Syslog の管理	システム設定の管理
トンネル設定値の設定	プロビジョニングの設定

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注）*読者に留意していただきたいことを示します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。*

「注意：」は、*注意が必要なことを示しています。*機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告：安全上の重要事項

危険の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

規制：追加情報および規制要件または顧客要件に準拠するために定められています。

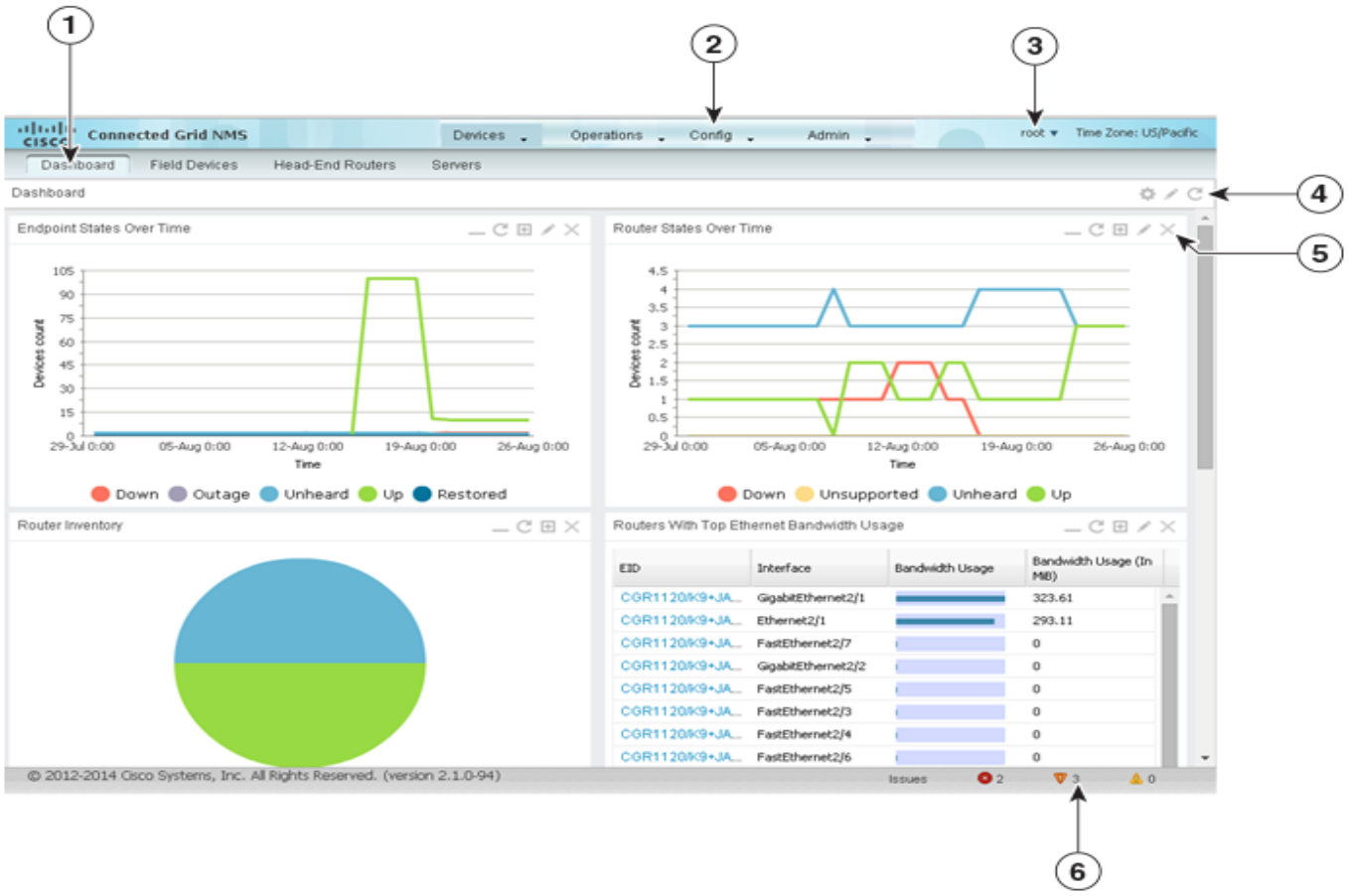
インターフェイスの概要

この項では、IoT FND GUI の一般的な概要を説明しており、次の内容が含まれています。

- 共通ページのコントロール
- アイコン
- メイン メニュー

IoT FND は、ユーザのログイン後にダッシュボードを表示します（図 4）。ダッシュボードの使用を参照してください。

図 4　　IoT FND ダッシュボード



1	サブメニュー タブ	4	ダッシュボードのタイトル バー ボタンには、次のものがあります。 ■ Settings ■ Interval ■ Refresh
2	メイン メニュー	5	ダッシュレット ボタン: ■ Show/Hide ■ Export ■ Refresh ■ Interval/Filter Applied ■ Close
3	[*<user name>*] メニュー	6	[Issues] ステータス バー

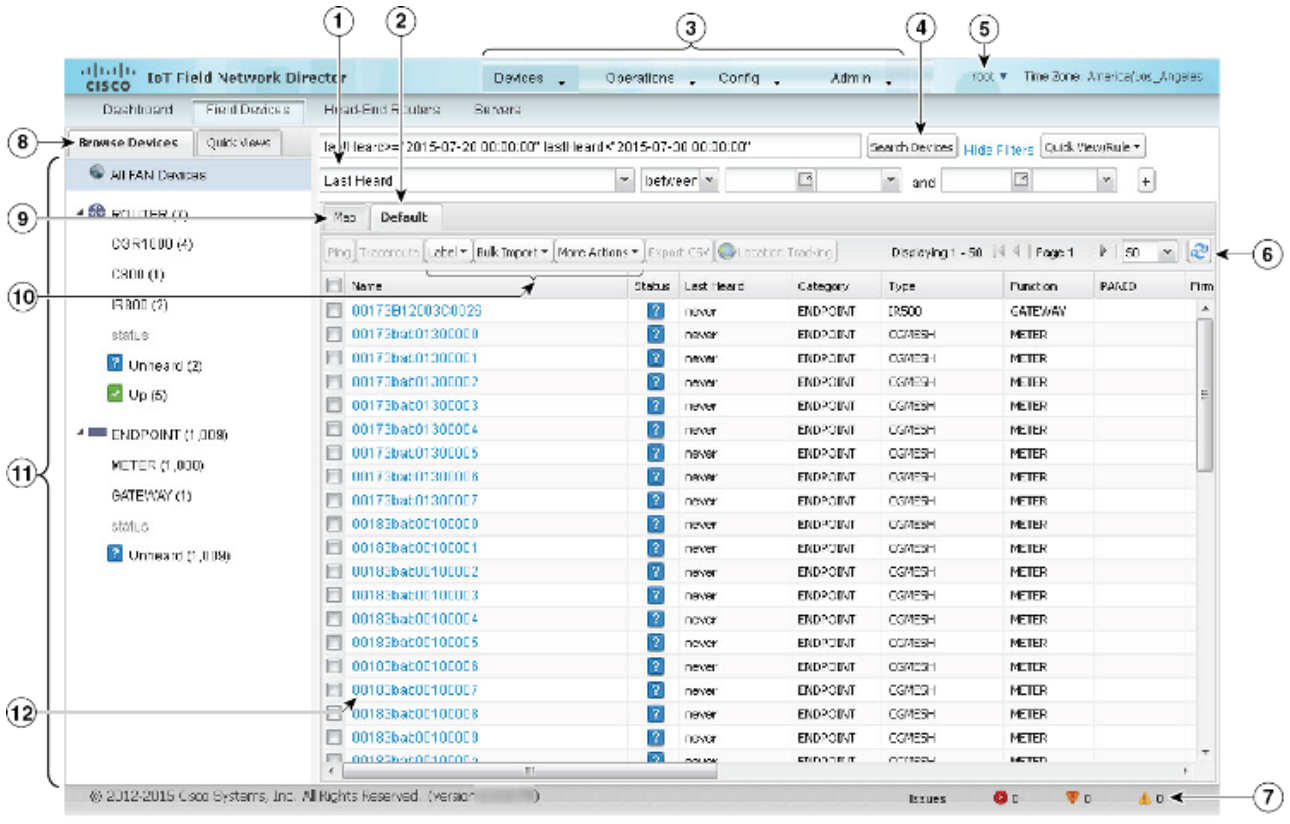
共通ページのコントロール

この項では、IoT FND の各ページのボタン、タブ、ユーザ入力フィールド、および選択可能な設定を説明しています。

メイン ウィンドウのナビゲート

図 5 に示すように、IoT FND ウィンドウの上部には、メイン メニュー [Devices]、[Operations]、[Config]、および [Admin] があります (3)。メニュー オプションを表示して選択するには、これらのメニューをロールオーバーします。サブメニューは、メイン メニューの下にタブとして表示されます。各ページには、そのページに固有の機能のコントロールがあります。

図 5　　メイン ウィンドウの要素



1	フィルタ ラベル ドロップダウン メニュー	7	[Issues] ステータス バー
2	デフォルトのリスト ビュー設定タブ	8	サブメニュー タブ
3	メイン メニュー	9	[Map] タブ
4	検索クエリ フィールド	10	デバイス管理ドロップダウン メニュー
5	[*<user name>*] メニュー	11	[Browse Devices] ペイン
6	[Refresh] ボタン	12	[Device Info] ページへのデバイス EID リンク

ユーザ プリファレンスの設定

メニュー バーの右上にある [*<user name>*] ドロップダウン メニューにアクセスして(5)、次のいずれかのオプションを設定または実行します。

- Preferences:ユーザ インターフェイスの表示設定を指定します。
- Change Password
- Time Zone
- Log Out

ビューの操作

デフォルトとカスタム グループのデバイスを表示するには、[Browse Devices] ペイン(11)を使用します。[Browse Devices] ペインの上部に、登録済みデバイスの総数が括弧で囲まれて表示されます。グループ内のデバイスの総数は、グループ名の横に括弧で囲まれて表示されます。

リスト表示はフィルタを使用して絞り込むことができます(フィルタを使用したデバイス表示の制御を参照)。組み込みフィルタは、[Browse Devices] ペインでデバイス グループをクリックすると自動的に導入されます。保存されたカスタム フィルタにアクセスするには、[Quick View] タブを使用します。

[Device Info] ページを表示するには、デバイス名または EID(要素識別子)リンク(12)をクリックします。ワーク オーダーを [Device Info] ページから直接生成し、ネットワーク内で応答するかどうかを確認するために、デバイスの ping などのいくつかのデバイス固有テストを実行できます。[Device Info] ページで [<<Back] リンクをクリックすると、デバイス EID リンクをクリックしたときに表示していたページに戻ります。リスト ビューを更新するには、任意のページ上で更新ボタン(6)をクリックします。

[User Preferences] の [Issues] ステータス バー(7)を有効にすると、アラーム状態別の問題の集計が、ブラウザ ウィンドウの下部に表示されます([Issues] ステータス バーでのデバイス重大度ステータスの表示を参照)。

タブの使用

ページを表示すると、メイン メニュー タブ(3)は暗く表示されます(たとえば、図 5 では、[Devices] が [Routers] ページのメイン メニューです)。各ページで、サブメニュー ページにアクセスするには、メイン メニュー バーの下のタブ(8)を使用します。ページを表示すると、タブは明るく表示されます(たとえば、図 5 の [Routers] タブ)。

各デバイス ページには、メイン ウィンドウに関連情報を表示するためのタブがあります(2 と 10)。アクティブなタブは、そのタブ上にマウスを移動させると明るく表示されます(たとえば、図 5 の [Default] タブ)。これらのタブは設定可能です(デバイス ビューの編集を参照)。[Default] タブのドロップダウン矢印をクリックすると、[Edit/Delete View] ダイアログが表示され、そこでリスト ビューのカラム表示を変更できます。リスト ビューはカラム幅も設定可能であり、列は昇順または降順でソートできます。

デバイスの使用

デバイスのチェックボックスをオンにすると、リストの上のドロップダウン メニューからデバイス管理を実行できます(7)。

- Label:デバイス ラベルを追加および削除します。
- Bulk Import:ラベル管理を実行し、デバイスのプロパティを変更し、デバイスを削除します。
- More Actions:ルータのワーク オーダーを作成し、ルータ メッシュ キーを更新し、メッシュ デバイスをブロックし、デバイスを削除します。

ページ ビューのナビゲート

デフォルトでは、デバイス管理ページは、ソート可能なテーブルにデバイスを表示するリスト ビューで表示されます。[Routers] ページおよび [Mesh] ページでは、[Map] タブ(9)を選択すると、GIS マップ上にデバイスが表示されます([Map] ビューでのルータの表示および[Map] ビューでのメッシュ エンドポイントの表示を参照)。

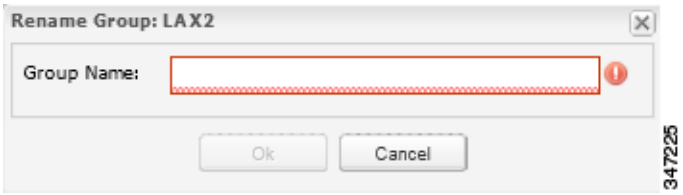
フィルタの処理

[Show Filters] リンクをクリックしてカスタム フィルタを作成し([Hide Filters] リンクは図 5 の同じ場所に表示される)、提供されるフィルタ パラメータを使用して(1)、[Search Devices] フィールドに適切な構文を作成します(4)。保存されたカスタム フィルタを表示するには、[Quick Views] タブをクリックします([Quick View] フィルタの作成および編集を参照)。

ユーザ入力フィールドの完成

図 6 は、ユーザ入力フィールドのエラーを示しています。IoT FND は赤色のアラート アイコンを表示し、フィールドを赤色で強調表示し、[OK] ボタンを無効にします。これらのエラーは、たとえば無効文字（@、#、!、または + など）を入力した場合や、入力が予期されているものの実行されていない場合などに発生します。

図 6　エラーになった [Group Name] ユーザ入力フィールド



アイコン

表 5 は、UI に表示されるアイコンをリストしています。

表 5　IoT FND アイコン

アイコン	説明
	このルータ アイコンは、CGR、ISR、IR（FAR）、および HER に使用されます。
	これはサーバ アイコンです。
	これは DA ゲートウェイ（IR500）デバイス アイコンです。
	これはメーター アイコンです。
	これは未定義のエンドポイント アイコンです。
	この Up アイコンは、デバイスが稼働しておりオンラインであることを示します。
	この Down アイコンは、デバイスがダウンしていることを示します。
	この未登録アイコンは、デバイスが IoT FND にまだ登録されていないことを示します。
	停止アイコンは、デバイスが停止していることを示します。
	復元済みアイコンは、デバイスが停止から回復したことを示します。

表 5　　IoT FND アイコン（続き）

アイコン	説明
	デフォルト グループ アイコンは、それが最上位のデバイス グループであることを示します。すべてのデバイスは、正常に登録されるとこのグループに表示されます。
	これはグループ追加アイコンです。
	これはグループ編集/削除アイコンです。
	[Events] ページで、このボタンをクリックすると、CSV ファイルへのイベント データのエクスポートが開始されます。
	グループ アイコンは、それがカスタム デバイス グループであることを示します。
	カスタム ラベル アイコンは、デバイスのグループを示します。デバイスを論理グループにソートするには、ラベルを使用します。ラベルはデバイス タイプには依存しません。デバイスはどのタイプであっても、どのラベルにでも属することができます。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。
	[Dashboard] ページで、このボタンをクリックすると、データ更新間隔が設定され、ダッシュレットが追加されます。
	[Dashboard] ページで、このボタンをクリックすると、CSV ファイルへのダッシュレット データのエクスポートが開始されます。
	[Dashboard] ページで、このボタンをクリックすると、ダッシュレット データが更新されます。
	[Dashboard] ページで、このボタンをクリックすると、データ取得間隔設定が変更され、フィルタがダッシュレットに追加されます。線グラフ ダッシュレットでは、このボタンで、データ取得間隔設定やフィルタにアクセスできるだけでなく、グラフ固有のデータ設定にもアクセスできます。フィルタが適用されると、このアイコンは緑色になります。
	ダッシュレット タイトル バーの [Dashboard] ページで、このボタンをクリックすると、ダッシュレットの表示/非表示が切り替わります。ダッシュレットが非表示のときには、ダッシュボードにタイトル バーのみが表示されます。
	[Map] ビューでは、これは RPL ツリーのルート デバイス アイコンです。これは、RPL ツリー ポーリングの設定のときの設定に従って、CGR またはメッシュ デバイスになります。色はデバイスのステータス（Up、Down、および Unheard）を表します。 RPL ツリー接続は、青色またはオレンジ色の線で表示されます。 ■　オレンジの線は、リンクが機能していることを示します。 ■　青の線は、リンクがダウンしていることを示します。
	マップ ビューでは、これはデバイス グループ アイコンです。色はデバイスのステータス（Up、Down、および Unheard）を表します。

表 5　　IoT FND アイコン（続き）

アイコン	説明
	[Events] ページと [Issues] ページ、および [Issues] ステータス バーでは、これらのアイコンはイベント重大度レベルを示しています。重大度は高いほうから低いほうに、次のものがあります。 ■ Critical ■ Major ■ Minor ■ Info 各イベント タイプには、プリセットの重大度レベルがあります。たとえば、Router Down イベントは、Major 重大度レベルのイベントです。
	[Firmware Update] ページで、ファームウェア更新を設定するには、この「インストールおよびリロード スケジュール」ボタンをクリックします。
	[Firmware Update] ページで、選択したイメージをファームウェア イメージ バックアップとして設定するには、この「バックアップとして設定」ボタンをクリックします。

メイン メニュー

この項では、ページの上部のタイトル バーから使用できる IoT FND の各メニューについて説明しています。

[Devices] メニュー

[Devices] メニューからは、ダッシュボードとデバイス管理ページにアクセスできます。

- ダッシュボード：このユーザ設定可能ページには、Connected Grid に関する情報が表示されます。
- Field Devices：このページには、グリッド内の登録済みルータとメッシュ エンドポイントのトップレベル ビューが表示されます。
- Head-End Routers：このページには、グリッド内の登録済み HER のトップレベル ビューが表示されます。
- Servers：このページには、ネットワーク内の IoT FND とデータベース サーバのトップレベル ビューが表示されます。

[Operations] メニュー

[Operations] メニューでは、次のタブにアクセスできます。

- Events：このページには、グリッド内で発生したイベントが表示されます。
- Issues：このページには、管理者によるクイック レビューと解決のために、未解決のネットワーク イベントが表示されます。
- Tunnel Status：このページには、プロビジョニングされたトンネルがリストされ、トンネルとそのステータスに関する情報が表示されます。
- Work Orders：ワーク オーダーを作成してモニタするには、このページを使用します。

[Config] メニュー

[Config] メニューからは、次のタブにアクセスできます。

- App Management（IOS CGR のみ）：アプリケーションを管理するには、このページを使用します。
- Device Configuration：デバイスのプロパティを設定するには、このページを使用します。
- Firmware Update：1 つまたは複数のデバイスへの新しいイメージのインストール、デバイスのファームウェア グループの変更、デバイス（ルータ、エンドポイント）上の現在のファームウェア イメージの表示、およびメッシュ エンドポイントに関するサブネット詳細の表示を実行するには、このページを使用します。
- Router File Management：デバイス ファイルのステータスを表示したり、FAR からのファイルのアップロードや削除を実行したりするには、このページを使用します。
- Rules：イベント条件やメトリックしきい値をチェックするためのルールを作成するには、このページを使用します。
- Tunnel Provisioning：デバイスのトンネルをプロビジョニングするには、このページを使用します。

[Admin] メニュー

[Admin] メニューは、システム設定とユーザ アカウントの管理のための 2 つのエリアに分割されています。

- アクセス管理のページ：
  - Password Policy：ユーザのパスワードが満たす必要があるパスワード条件を設定するには、このページを使用します。
  - Remote Authentication：IoT-DM ユーザのリモート認証を設定するには、このページを使用します。
  - Roles：ユーザ ロールを定義するには、このページを使用します。
  - Users：ユーザ アカウントを管理するには、このページを使用します。
- システム管理のページ：
  - Active Sessions：IoT FND セッションをモニタするには、このページを使用します。
  - Audit Trail：ユーザ アクティビティを追跡するには、このページを使用します。
  - Certificates：IoT FND が使用する CSMP（CoAP Simple Management Protocol）、IoT-DM、および Web ブラウザの証明書を管理するには、このページを使用します。
  - [Data Retention]：このページを使用して、NMS データベースにイベント、問題、およびメトリック データを保持する日数を決定します。
  - License Center：ライセンス ファイルを表示および管理するには、このページを使用します。
  - Logging：さまざまなログ カテゴリおよびダウンロード ログのログ レベルを変更するには、このページを使用します。
  - Provisioning Settings：IoT FND URL の設定や、動的ホスト構成プロトコル v4（DHCPv4）プロキシ クライアントと DHCPv6 プロキシ クライアントの設定を行い、CGR と ASR との間のトンネルを作成するには、このページを使用します。
  - Server Settings：このページを使用して、サーバ設定を表示および管理します。
  - Syslog Settings：このページを使用して、Syslog 設定を表示および管理します。

Cisco IoT FND のインストール

ここでは、IoT FND と関連ソフトウェアのインストール方法について説明します。具体的な内容は次のとおりです。

- IoT FND をインストールする前に
- IoT FND データベースのインストールと設定
- IoT FND のインストールおよびセットアップ
- IoT FND TPS プロキシのインストールと設定
- Dual-PHY 用の IoT FND の設定
- IoT FND データベースのバックアップと復元
- ESX 5.x での IoT FND/Oracle/TPS 仮想マシンの展開

IoT FND をインストールする前に

次の項の手順を使用して、IoT FND インストールの準備を行います。

- IoT FND マップ ビューの要件
- システム要件
- IoT FNDおよび CNR のライセンスの取得
- Oracle のインストールに必要な Linux パッケージのインストール
- IoT FND RPM パッケージの取得
- NTP サービスの設定
- IoT FND のインストールの概要

IoT FND マップ ビューの要件

任意のデバイス タブで、メイン ペインの [Map] ボタンをクリックして、デバイス ロケーションの GIS マップを表示します。その [Map View] ペインで、IoT FND は、GIS マップを使用してデバイスの場所を表示します。ただし、この機能を使用するには、すべての IoT FND オペレータ システムがシスコが提供する GIS マップ タイル サーバにアクセスできるように、事前にファイアウォールを設定する必要があります。GIS マップ タイル サーバへのアクセスが許可されているのは、IoT FND オペレータ ブラウザだけです。

(注) オペレータ ブラウザは他の Google サイトにアクセスできません。IoT FND アプリケーション サーバにはインターネット アクセスは必要ありません。

また、完全修飾ドメイン名(FQDN)を各 IoT FND サーバのインストールに割り当て、ask-fnd-pm-external@cisco.com でシスコに以下を提供する必要があります。

- IoT FND インストール環境(テストおよび実稼働)の数
- IoT FND サーバの FQDN

- クラスタ展開の場合、展開での任意のロード バランサの FQDN

(注) FQDN は、プロビジョニングと、ライセンス付与された Cisco IoT FND インストールへのアクセスを認証して、Enterprise Google Map への API コールを行ってマップ タイルをダウンロードするためにのみ使用されます。Google マップ タイルを取得するために、ユーティリティ運用データまたは資産情報が使用(つまり、インターネットを介して送信)されることはありません。マップ タイルは、地理的な位置情報だけを使用して取得されます。

FQDN 情報の例

たとえば、非クラスタのインストールのドメイン名が UtilityA.com でホスト名が cgnms1、FQDN が cgms1.UtilityA.com とします。ask-cgnms-pm@cisco.com に電子メールを送信する際には、FQDN、cgms1.UtilityA.com を含めます。

1 つ以上の IoT FND サーバと loadbalancer-vip という FQDN を持つロード バランサがあるクラスタ展開では、トラフィックを cgnms-main または cnms-dr クラスタに向けます(DR インストール)。ask-cgnms-pm@cisco.com に電子メールを送信する際には、FQDN、loadbalancer-vip.UtilityA.com を含めます。

システム要件

表 1 に、このリリースに関連付けられている必要なハードウェアとソフトウェアのバージョンを示します。

(注) 大規模なシステムについては、表 2 と表 3 のスケール要件を参照してください。

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco IoT FND アプリケーション サーバ(またはハードウェアとソフトウェアの最小要件を満たす同等のシステム)	■ プロセッサ – Intel Xeon x5680 2.27 GHz (64 ビット) – 4 個の CPU – RAM:16 GB ■ ディスク領域:100 GB ■ ハードウェア セキュリティ モジュール(HSM) または ソフトウェア セキュリティ モジュール(SSM)	■ すべてのパッケージ(ソフトウェア開発と Web サーバ)がインストールされた Red Hat Enterprise Linux 6.4 以降(64 ビット版) 推奨されるアプリケーション サーバのリソース割り当てプロファイルについては、表 3(26 ページ)を参照してください。 ■ インターネット接続 クライアントのブラウザから IoT FND にアクセスすると、ブラウザはインターネットに接続して、GIS マップ プロバイダーから必要なデータ ファイルをダウンロードします。 ■ メッシュ エンドポイント セキュリティに SafeNet を使用するためのライセンス (注) IoT FNDソフトウェア バンドルには、必要な Java のバージョンが含まれています。
Cisco IoT FND TPS プロキシ	■ プロセッサ – Intel Xeon x5680 2.27 GHz (64 ビット) – 2 個の CPU ■ RAM:4 GB ■ ディスク領域:25 GB	■ すべてのパッケージ(ソフトウェア開発と Web サーバ)がインストールされた Red Hat Enterprise Linux 6.4 以降 ■ インターネット接続 (注) IoT FND ソフトウェア バンドルには、必要な Java のバージョンが含まれています。

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
IoT FND のデータベース サーバ ハードウェアの最小要件で 25 ルータ/10,000 エンドポイントに拡張できます。追加で拡張可能なサイズについては、「リソース管理の注意事項」を参照してください。	■ プロセッサ – Intel Xeon x5680 3.33 GHz（64 ビット） ■ 2 個の CPU ■ RAM：16 GB ■ ディスク領域：100 GB（Oracle 12c のインストール時には 120 GB）	（注）IoT FND 3.2.x は、次に示す Oracle リリースの両方をサポートします。 ■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production（パッチ 20830993） ■ Oracle 11g Enterprise Edition（11.2.0.3 64 ビット バージョンのみ） （注）Oracle をインストールする前に、「Oracle のインストールに必要な Linux パッケージのインストール」に記載されている Linux パッケージをインストールします。 推奨される Oracle データベース サーバのリソース割り当てプロファイルについては、表 2（26 ページ）を参照してください。 ■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Linux 6.4 以降（64 ビット版）
Cisco IoT FND クライアント	クライアントが IoT FND アプリケーション サーバに接続して IoT FND を表示するには、次の最小要件を満たしている必要があります。 ■ Windows 7 または Win2000 R2 サーバ ■ RAM：8 GB ■ プロセッサ：2 GHz ■ 解像度：1024 x 768	■ Adobe Flash バージョン 9.0.115 以降（チャートを表示するために必要） ■ サポートされるブラウザ： – Internet Explorer（IE）：11.0 – Mozilla Firefox：3.5 以降 – IE 11.0 が機能する Windows 7

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco Network Registrar（CNR）（DHCP サーバとして使用）	サーバは、次の最小要件を満たしている必要があります。 ■ ディスクの空き容量：146 GB ■ RAM：4 GB（小規模ネットワーク）、8 GB（平均的なネットワーク）、16 GB（大規模なネットワーク） ■ ハード ドライブ： – SATA ドライブ（7500 RPM ドライブ、500 リース/秒以上） *または* – SAS ドライブ（15K RPM ドライブ、1000 リース/秒以上）	Cisco Network Registrar、ソフトウェア リリース 8.2 をサーバにインストールする前に、次のソフトウェア環境が存在している必要があります。 ■ オペレーティング システム：Windows Server 2000 ■ Development Kit（JDK）Java SE Runtime Environment（JRE）8.0（1.8.0_65-b17）または同等の Java Development Kit（JDK）。 ■ ユーザ インターフェイス：Web ブラウザと、コマンドライン インターフェイス（CLI）（次に示すブラウザ バージョン）： – Internet Explorer（IE）11.0、Mozilla Firefox 3.0 以降 ■ CNR ライセンス。必要なライセンスについては、シスコ パートナーにお問い合わせください。
IoT Device Manager（IoT-DM または Device Manager）	Device Manager を実行しているラップトップには、以下が必要です。 ■ Microsoft Windows 7 Enterprise ■ 2 GHz 以上のプロセッサ（推奨） ■ 1 GB 以上の RAM（大きくなる可能性のあるログ ファイル処理用） ■ Wi-Fi またはイーサネット インターフェイス ■ 4 GB のディスク ストレージ領域 ■ Windows ログインが有効になっていること ■ ユーティリティにより署名された認証局（CA）とルータの認証用のクライアント証明書（IT 部門から入手） ■ Device Manager のラップトップ セキュリティを強化するための顧客固有の IT セキュリティ	■ バージョン 5.0.0.16
Cisco 1000 シリーズ Connected Grid ルータ	–	■ Cisco IOS Release 15.6.3M1b ■ Cisco CG-OS Release CG4(5)
Cisco ISR 800 シリーズ サービス統合型ルータ（C800）	–	■ Cisco IOS Release 15.6.3M1

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco 800 シリーズ アクセス ポイント（AP800）	-	■ AP802：ap802-k9w7-tar.153-3.JBB.tar ■ AP803：ap1g3-k9w7-tar.153-3.JBB2.tar
Cisco 800 シリーズ産業用サービス統合型ルータ（IR800）	-	■ Cisco IOS Release 15.6.3M1b
Cisco 3900 シリーズ サービス統合型ルータ（ISR）	-	■ Cisco IOS Release 15.4(3)M ■ Cisco IOS Release 15.4(2)T
Cisco ASR 1001 または 1002 アグリゲーション サービス ルータ（ASR）はヘッドエンド ルータとして機能します。	-	■ Cisco IOS XE Release 3.17.02.S Flex トンネル用（IOS） ■ Cisco IOS XE Release 3.11S ポイントツーポイント トンネル用（CG-OS）
Cisco 500 シリーズ Wireless Personal Area Network（WPAN）産業用ルータ（IR500）	-	■ Cisco IR509、DA ゲートウェイ デバイス：ファームウェア バージョン 5.6.10 ■ Cisco IR529、Range Extender：ファームウェア バージョン 5.6.10
（注）異なるリリースの ASR と ISR はネットワーク上に共存できます。		
Cisco Connected Grid CG-Mesh Module とサポートされるエンドポイント	-	■ ファームウェア バージョン 5.6.10 以下と通信する場合 CGR 1000 または Cisco ASR、およびこれらのリリース ノートでこれらのルータに推奨されている Cisco IOS ソフトウェアの最小バージョン
Cisco Connected Grid RF メッシュ エンドポイント		■ ファームウェア バージョン 5.6.10（IR500 と通信する場合）
Cisco 800 シリーズ産業用サービス統合型ルータ（IR800）用に LoRAWAN（Long Range Wide Area Network）インターフェイス モジュール	-	■ Cisco IOS 15.6.3M1b
ハードウェア セキュリティ モジュール（HSM）	クライアント ソフトウェアが IoT FND アプリケーション サーバにインストールされた Luna SA アプライアンス	Luna SA アプライアンス： ■ リリース 6.10.2 ファームウェア （注）上位のバージョンを実行できるかどうかは、SafeNet にお問い合わせください。 ■ リリース 5.4.7-1 ソフトウェアとセキュリティ パッチ Luna SA クライアント ソフトウェア： ■ リリース 5.4.7-1 ソフトウェア
ソフトウェア セキュリティ モジュール（SSM）	■ RAM：8 GB ■ プロセッサ：2 GHz ■ 2 個の CPU	■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Enterprise Linux 6.4 または 7.1（64 ビット版）

(注) IoT FND サーバ クラスタを展開している場合、クラスタ内のすべてのノードを同じようなハードウェアで実行する必要があります。さらに、すべてのノードで同じバージョンの IoT FND を実行する必要があります。

リソース管理の注意事項

仮想マシン設定のワークロード特性は重要です。同じ物理ホスト上で複数の VM を使用する場合、個々の VM が他の VM のパフォーマンスに影響を及ぼさないようにリソースを割り当てます。たとえば、8 CPU のホストで 4 つの VM を割り当てるには、1 つ(以上)の VM がすべてのリソースを使用しないように、8 つの CPU すべてを割り当てないようにします。

表 2(26 ページ)では、CPU、メモリ、ディスク領域などの重要なリソース パラメータの Oracle データベース サーバの使用プロファイルの例がリストされています。

(注) 表 2 に関しては、次の点に注意してください。Oracle が仮想マシン(VM)にバンドルされている IOTFND SKU (R-IOTFND-V-K9)をインストールする場合、サポートされるルータの最大数は 1000 で、サポートされるエンドポイントの最大数は 250,000 です。

表 2　Oracle DB サーバ ハードウェア要件のプロファイル例

ノード (ルータ/エンドポイント)	CPU (仮想コア)	メモリ (RAM GB)	ディスク領域(GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	8	32	500
1,000/1,000,000	12	48	1000
2,000/2,000,000	16	64	1000
5,000/5,000,000	20	96	1000

表 3(26 ページ)では、CPU、メモリ、ディスク領域などの重要なリソース パラメータの IoT FND アプリケーション サーバの使用プロファイルの例がリストされています。

表 3　アプリケーション サーバのハードウェア要件のプロファイル例

ノード (ルータ/エンドポイント)	CPU (仮想コア)	メモリ (RAM GB)	ディスク領域(GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000[1]	8	16	500
5,000/5,000,000[1]	8	16	500

1. クラスタ構成のインストール。

(注) すべての展開に RAID 10 を強くお勧めします。

ルータのみの展開の場合

表 4 と表 5 の情報は、ルータのみの展開に適用されます。

表 4　　ルータおよび LoRa モジュールのアプリケーション サーバのハードウェア要件のプロファイル例

ノード（IR800/LoRa モジュール）	CPU（仮想コア）	メモリ（RAM GB）	ディスク領域（GB）
10,000/30,000	4	24	100

表 5　　ルータおよび LoRa モジュールのデータベース サーバのハードウェア要件のプロファイル例

ノード（IR800/LoRa モジュール）	CPU（仮想コア）	メモリ（RAM GB）	ディスク領域（GB）
10,000/30,000	6	32	500

IoT FNDおよび CNR のライセンスの取得

- IoT FND および CNR を使用するために必要なライセンスを取得するには、シスコ パートナーにお問い合わせください。
- メッシュ エンドポイント セキュリティの HSM として SafeNet を使用するため、ライセンスを取得します。

Oracle のインストールに必要な Linux パッケージのインストール

Oracle データベースをインストールする前に、次のパッケージをこの順序でインストールします。

1. libaio-devel-0.3.106-5.i386.rpm
2. libaio-devel-0.3.106-5.x86_64.rpm
3. sysstat-7.0.2-11.el5.x86_64.rpm
4. unixODBC-libs-2.2.11-10.el5.i386.rpm
5. unixODBC-libs-2.2.11-10.el5.x86_64.rpm
6. unixODBC-2.2.11-10.el5.i386.rpm
7. unixODBC-2.2.11-10.el5.x86_64.rpm
8. unixODBC-devel-2.2.11-10.el5.i386.rpm
9. unixODBC-devel-2.2.11-10.el5.x86_64.rpm

IoT FND RPM パッケージの取得

IoT FND システムをインストールして設定する前に、次のパッケージがあることを確認します。

RPM パッケージ	説明
cgms-*version_number*.x86_64.rpm	IoT FND インストーラが含まれています。これが IoT FND アプリケーション サーバそのものを含むメインの RPM です。IoT FND アプリケーション サーバにこのパッケージをインストールします。
cgms-oracle-*version_number*.x86_64.rpm	IoT FND Oracle データベースを作成するためのスクリプトとツールが含まれています。このパッケージには、Oracle データベース テンプレートと、管理スクリプトが含まれています。IoT FND データベース サーバ システムにこのパッケージをインストールします。
cgms-tools-*version_number*.x86_64.rpm	オプションのコマンドライン ツールがいくつか含まれています。必要に応じて、IoT FND アプリケーション サーバが動作しているシステムにこのパッケージをインストールします。
cgms-ssm-*version_number*.x86_64.rpm	ソフトウェア セキュリティ モジュール(SSM)が含まれています。IoT FND アプリケーション サーバが動作しているシステムにこのパッケージをインストールします。
cgms-tpsproxy-*version_number*.x86_64.rpm	TPS プロキシ アプリケーションが含まれます。IoT FND TPS プロキシ システムにこのパッケージをインストールします。

NTP サービスの設定

IoT FND の展開のすべての RHEL サーバ(IoT FND を実行するすべてのサーバを含む)の NTP サービスを有効化するように設定し、システムの他のサーバと同じタイム サーバを使用するように設定します。

注意: 証明書が生成される前に、すべてのシステム コンポーネントのクロックを同期します。

RHEL サーバで NTP を設定するには、次の手順を実行します。

1. /etc/ntp.conf ファイルを設定します。

   次に例を示します。

   ```
   cat /etc/ntp.conf
   ...
   # Use the same NTP servers on all our Connected Grid systems.
   server 0.ntp.example.com
   server 1.ntp.example.com
   server 2.ntp.example.com
   ...
   ```

2. NTP デーモンを再起動して、ブート時に実行されるように設定されていることを確認します。

   ```
   service ntpd restart
   chkconfig ntpd on
   ```

3. NTP デーモンのステータスを確認して、設定の変更を確認します。

この例では、192.0.2.1 でシステムがローカル NTP サーバになるように設定されていることを示しています。このサーバは、10.0.0.0 で NTP サーバを使用して時刻を同期します。

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.1       198.51.100.1    3 u    309 1024  377    0.694    0.899   0.435
 LOCAL(0)        .LOCL.          10 l    36   64  377    0.000    0.000   0.001
```

RHEL サーバでの NTP の設定については、RHEL のマニュアルを参照してください。

IoT FND のインストールの概要

IoT FND をインストールするには、次の手順を実行します。

1. IoT FND データベースのインストールと設定。
2. IoT FND のインストールおよびセットアップ。
3. IoT FND TPS プロキシのインストールと設定。

IoT FND データベースのインストールと設定

次の手順を実行して、IoT FND のインストールを完了します。

- インストールと設定の概要
- Oracle データベースのダウンロードと解凍
- Oracle データベース インストーラの実行
- IoT FND データベースの設定
- IoT FND データベースのその他のトピック

インストールと設定の概要

ここでは、IoT FND の展開の概要について説明します。

- シングルサーバの展開
- ハイ アベイラビリティ展開

シングルサーバの展開

シングルサーバ データベースの展開に IoT FND データベースをインストールして設定するには、次の手順を実行します。

1. データベース サーバにログインします。
2. Oracle データベースのダウンロードと解凍。
3. Oracle データベース インストーラの実行。
4. IoT FND データベースの設定。

ハイ アベイラビリティ展開

HA 用に IoT FND データベースをインストールして設定するには、次の手順を実行します。

1. プライマリ IoT FND データベース サーバにログインします。
2. Oracle データベースのダウンロードと解凍。
3. Oracle データベース インストーラの実行。
4. スタンバイ データベース サーバにログインします。
5. Oracle データベースのダウンロードと解凍。
6. Oracle データベース インストーラの実行。

7. HA 用の IoT FND データベースの設定。

Oracle データベースのダウンロードと解凍

Oracle データベースをダウンロードするには、次の手順を実行します。

1. root としてサーバにログインします。
2. Oracle 11g Enterprise Edition（11.2.0.3 64 ビット）または Oracle12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production（パッチ 20830993）をダウンロードします。
3. Oracle データベース ソフトウェアのインストール時に表示関連のエラーを回避するには、root として次のコマンドを実行します。

```
# xhost + local:oracle
```

4. **oracle** ユーザと **dba** グループを作成します。

```
# groupadd dba
# adduser -d /home/oracle -g dba -s /bin/bash oracle
```

5. Oracle データベースの zip アーカイブを解凍します。

```
p10404530_112030_Linux-x86-64_1of7.zip
p10404530_112030_Linux-x86-64_2of7.zip
p10404530_112030_Linux-x86-64_3of7.zip
p10404530_112030_Linux-x86-64_4of7.zip
p10404530_112030_Linux-x86-64_5of7.zip
p10404530_112030_Linux-x86-64_6of7.zip
p10404530_112030_Linux-x86-64_7of7.zip
```

Oracle データベース インストーラの実行

（注）Oracle インストーラを実行する前に、ファイアウォールを無効にします。

Oracle データベースをインストールするには、次の手順を実行します。

1. ユーザ **oracle** に切り替え、Oracle データベースのインストーラを実行します。

```
# su - oracle
# setenv DISPLAY <desktop>
# path_to_DB_installation_folder/database/runInstaller
```

2. [Yes] をクリックし、[Next] をクリックします。
3. [Install database software only] をクリックし、[Next] をクリックします。
4. [Single instance database installation] をクリックし、[Next] をクリックします。
5. データベースを実行する言語として [English] を選択し、[Next] をクリックします。
6. [Enterprise Edition (4.29GB (Oracle 11g)] または [6.4GB (Oracle12c)] をクリックし、[Next] をクリックします。
7. 次の 2 つのデフォルトのインストール値、Oracle ベースおよびソフトウェアの場所（**11.2.0** または **12.1.0**）を選択し、[Next] をクリックします。
   - Oracle ベース：**/home/oracle/app/oracle**
   - ソフトウェアの場所：**/home/oracle/app/oracle/product/11.2.0/dbhome_1**
   - ソフトウェアの場所：**/home/oracle/app/oracle/product/12.1.0/dbhome_1**

後で Oracle ベースとソフトウェアの場所のプロパティの値に基づいて環境変数 ORACLE_BASE と ORACLE_HOME を作成します。

8. [Create Inventory] ページで、デフォルト値を維持し、[Next] をクリックします。
   - インベントリ ディレクトリ：**/home/oracle/app/oraInventory**
   - oraInventory_Group 名：**dba**

9. [Privileged Operating System Groups] ページで、デフォルト値を維持し、[Next] をクリックします。
   - データベース管理者（OSDBA）グループ：**dba**
   - データベース オペレータ（OSOPER）グループ：**dba**

   データベースのバックアップとリカバリ（OSBACKUPDBA）グループ：**dba**（12c のみ）
   - データ ガード管理（OSDGDBA）グループ：**dba**（12c のみ）
   - 暗号化キー管理の管理（OSKMDBA）グループ：**dba**（12c のみ）

10. （オプション）[Perform Prerequisite Checks] ページで、必要なソフトウェアをインストールするか、提供されるスクリプトを実行します。

    システム カーネルの設定に基づいて、インストーラによって追加のソフトウェアのインストールが求められる場合があります。また、スクリプトを実行してシステムを設定し、データベースのインストールを完了するように指示される場合があります。

    (注) 不足しているパッケージが示されない場合、または「This is a prerequisite condition to test whether the package “ksh” is available on the system」というメッセージが表示された場合は、[Ignore All] ボックスをオンにします。

11. 不足しているパッケージをインストールした後、[Fix & Check Again] をクリックします。

    すべての要件を満たすまでこれを続けます。

    注意： このページのエラーは無視しないでください。データベースのインストール中にエラーが発生すると、IoT FND が適切に機能しない可能性があります。

12. [Next] をクリックします。

13. [Summary] ページで、データベース設定を確認し [Finish]（11g）または [Install]（12c）をクリックして、インストール プロセスを開始します。

14. プロンプトで、提供される構成スクリプトを実行します。

    インストーラはユーザ *oracle* で実行するため、ルート権限を必要とする特定のインストール操作は実行できません。これらの操作を実行するため、インストール プロセスを完了するためのスクリプトを実行するように求められます。プロンプトが表示されたら、ターミナル ウィンドウを開き、root としてスクリプトを実行します。

15. 正常にインストールされたら、[Finish] ページで [Close] をクリックします。

    (注) Oracle 12c の新規インストールまたは Oracle 11g からのアップグレードを実行する場合には、Oracle 12c パッチ 20830993 をインストールする**必要**があります。(必須) 12c パッチのインストール に進みます。

(必須) 12c パッチのインストール

Oracle 12c データベースの新規インストールと Oracle 11g からのアップグレードにはすべて、12c パッチをインストールする必要があります。

パッチをインストールするには、次の手順を実行します。

1. IoT FND アプリケーションが実行されている場合は停止します。
2. Oracle サービスが実行されている場合は停止します。
3. 次のコマンドを実行して、インストール済みの Oracle ソフトウェア コンポーネントとパッチのインベントリを確認します。この段階ではパッチは適用されていません。最後に「*There are no interim patches installed in this Oracle Home*」が表示されます。

```
/home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details

Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory   from           :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location
:/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_10-37-50AM_1.log

Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_10-37-50
AM.txt
--------------------------------------------------------------------------------

Installed Top-level Products (1):
Oracle Database 12c                                                  12.1.0.2.0
There are 1 products installed in this Oracle Home.
Installed Products (135):
Assistant Common Files                                               12.1.0.2.0
Buildtools Common Files                                              12.1.0.2.0
Cluster Verification Utility Common Files                            12.1.0.2.0
Database Configuration and Upgrade Assistants                        12.1.0.2.0
Database Migration Assistant for Unicode                             12.1.0.2.0
Database SQL Scripts                                                 12.1.0.2.0
Database Workspace Manager                                           12.1.0.2.0
DB TOOLS Listener                                                    12.1.0.2.0
Deinstallation Tool                                                  12.1.0.2.0
Enterprise Edition Options                                           12.1.0.2.0
Expat libraries                                                       2.0.1.0.2
Generic Connectivity Common Files                                    12.1.0.2.0
Hadoopcore Component                                                 12.1.0.2.0
HAS Common Files                                                     12.1.0.2.0
HAS Files for DB                                                     12.1.0.2.0
Installation Common Files                                            12.1.0.2.0
Installation Plugin Files                                            12.1.0.2.0
Installer SDK Component                                              12.1.0.2.0J
Accelerator (COMPANION)                                              12.1.0.2.0
Java Development Kit                                                 1.6.0.75.0
LDAP Required Support Files                                          12.1.0.2.0
OLAP SQL Scripts                                                     12.1.0.2.0
Oracle Advanced Security                                             12.1.0.2.0
Oracle Application Express                                           12.1.0.2.0
Oracle Bali Share                                                    11.1.1.6.0
Oracle Call Interface (OCI)                                          12.1.0.2.0
Oracle Clusterware RDBMS Files                                       12.1.0.2.0
```

```
Oracle Configuration Manager                                    10.3.8.1.1
Oracle Configuration Manager Client                             10.3.2.1.0
Oracle Configuration Manager Deconfiguration                    10.3.1.0.0
Oracle Containers for Java                                      12.1.0.2.0
Oracle Context Companion                                        12.1.0.2.0
Oracle Core Required Support Files                              12.1.0.2.0
Oracle Core Required Support Files for Core DB                  12.1.0.2.0
Oracle Core XML Development Kit                                 12.1.0.2.0
Oracle Data Mining RDBMS Files                                  12.1.0.2.0
Oracle Database 12c                                             12.1.0.2.0
Oracle Database 12c                                             12.1.0.2.0
Oracle Database 12c Multimedia Files                            12.1.0.2.0
Oracle Database Deconfiguration                                 12.1.0.2.0
Oracle Database Gateway for ODBC                                12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder      12.1.0.2.0
Oracle Database User Interface                                  11.0.0.0.0
Oracle Database Utilities                                       12.1.0.2.0
Oracle Database Vault option                                    12.1.0.2.0
Oracle DBCA Deconfiguration                                     12.1.0.2.0
Oracle Extended Windowing Toolkit                               11.1.1.6.0
Oracle Globalization Support                                    12.1.0.2.0
Oracle Globalization Support                                    12.1.0.2.0
Oracle Globalization Support For Core                           12.1.0.2.0
Oracle Help for Java                                            11.1.1.7.0
Oracle Help Share Library                                       11.1.1.7.0
Oracle Ice Browser                                              11.1.1.7.0
Oracle Internet Directory Client                                12.1.0.2.0
Oracle Java Client                                              12.1.0.2.0
Oracle Java Layout Engine                                       11.0.0.0.0
Oracle JDBC Server Support Package                              12.1.0.2.0
Oracle JDBC/OCI Instant Client                                  12.1.0.2.0
Oracle JDBC/THIN Interfaces                                     12.1.0.2.0
Oracle JFC Extended Windowing Toolkit                           11.1.1.6.0
Oracle JVM                                                      12.1.0.2.0
Oracle JVM For Core                                             12.1.0.2.0
Oracle Label Security                                           12.1.0.2.0
Oracle LDAP administration                                      12.1.0.2.0
Oracle Locale Builder                                           12.1.0.2.0
Oracle Message Gateway Common Files                             12.1.0.2.0
Oracle Multimedia                                               12.1.0.2.0
Oracle Multimedia Client Option                                 12.1.0.2.0
Oracle Multimedia Java Advanced Imaging                         12.1.0.2.0
Oracle Multimedia Locator                                       12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files           12.1.0.2.0
Oracle Multimedia Locator RDBMS Files                           12.1.0.2.0
Oracle Net                                                      12.1.0.2.0
Oracle Net Java Required Support Files                          12.1.0.2.0
Oracle Net Listener                                             12.1.0.2.0
Oracle Net Required Support Files                               12.1.0.2.0
Oracle Net Services                                             12.1.0.2.0
Oracle Netca Client                                             12.1.0.2.0
Oracle Notification Service                                     12.1.0.2.0
Oracle Notification Service (eONS)                              12.1.0.2.0
Oracle Notification Service for Instant Client                  12.1.0.2.0
Oracle ODBC Driver                                              12.1.0.2.0
Oracle ODBC Driverfor Instant Client                            12.1.0.2.0
Oracle OLAP                                                     12.1.0.2.0
Oracle OLAP API                                                 12.1.0.2.0
Oracle OLAP RDBMS Files                                         12.1.0.2.0
Oracle One-Off Patch Installer                                  12.1.0.1.2
Oracle Partitioning                                             12.1.0.2.0
Oracle Programmer                                               12.1.0.2.0
Oracle Quality of Service Management (Client)                   12.1.0.2.0
```

```
Oracle R Enterprise Server Files                                   12.1.0.2.0
Oracle RAC Deconfiguration                                         12.1.0.2.0
Oracle RAC Required Support Files-HAS                              12.1.0.2.0
Oracle Real Application Testing                                    12.1.0.2.0
Oracle Recovery Manager                                            12.1.0.2.0
Oracle Security Developer Tools                                    12.1.0.2.0
Oracle Spatial and Graph                                           12.1.0.2.0
Oracle SQL Developer                                               12.1.0.2.0
Oracle Starter Database                                            12.1.0.2.0
Oracle Text                                                        12.1.0.2.0
Oracle Text ATG Language Support Files                             12.1.0.2.0
Oracle Text for Core                                               12.1.0.2.0
Oracle Text Required Support Files                                 12.1.0.2.0
Oracle Universal Connection Pool                                   12.1.0.2.0
Oracle Universal Installer                                         12.1.0.2.0
Oracle USM Deconfiguration                                         12.1.0.2.0
Oracle Wallet Manager                                              12.1.0.2.0
Oracle XML Development Kit                                         12.1.0.2.0
Oracle XML Query                                                   12.1.0.2.0
oracle.swd.oui.core.min                                            12.1.0.2.0
Parser Generator Required Support Files                            12.1.0.2.0
Perl Interpreter                                                   5.14.1.0.0
Perl Modules                                                       5.14.1.0.0
PL/SQL                                                             12.1.0.2.0
PL/SQL Embedded Gateway                                            12.1.0.2.0
Platform Required Support Files                                    12.1.0.2.0
Precompiler Common Files                                           12.1.0.2.0
Precompiler Common Files for Core                                  12.1.0.2.0
Precompiler Required Support Files                                 12.1.0.2.0
Precompilers                                                       12.1.0.2.0
RDBMS Required Support Files                                       12.1.0.2.0
RDBMS Required Support Files for Instant Client                    12.1.0.2.0
RDBMS Required Support Files Runtime                               12.1.0.2.0
Required Support Files                                             12.1.0.2.0
Sample Schema Data                                                 12.1.0.2.0
Secure Socket Layer                                                12.1.0.2.0
SQL*Plus                                                           12.1.0.2.0
SQL*Plus Files for Instant Client                                  12.1.0.2.0
SQL*Plus Required Support Files                                    12.1.0.2.0
SQLJ Runtime                                                       12.1.0.2.0
SSL Required Support Files for InstantClient                       12.1.0.2.0
Tracle File Analyzer                                               12.1.0.2.0
XDK Required Support Files                                         12.1.0.2.0
XML Parser for Java                                                12.1.0.2.0
XML Parser for Oracle JVM                                          12.1.0.2.0
There are 135 products installed in this Oracle Home.

There are no Interim patches installed in this Oracle Home.
--------------------------------------------------------------------------------
```

4. パッチを適用します。

   a. データベース マシンで、パッチ ファイル "p20830993_121020_Linux-x86-64.zip" をコピーします。

   b. 要件のチェックを実行します。これにパスする必要があります。

```
$ cd /home/oracle/patches/20830993/
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch prereq
CheckConflictAgainstOHWithDetail -ph ./
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

PREREQ session
```

```
Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
   from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location :/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtool
logs/opatch/opatch2016-02-25_10-48-48AM_1.log

Invoking prereq "checkconflictagainstohwithdetail"

Prereq "checkConflictAgainstOHWithDetail" passed.

OPatch succeeded.
```

c. パッチを適用します。

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch apply
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory   from           :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location:
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/20830993_Feb_25_2016_10_53_25/ap
ply2016-02-25_10-53-25AM_1.log

Applying interim patch '20830993' to OH '/home/oracle/app/oracle/product/12.1.0/dbhome_1'
Verifying environment and performing prerequisite checks...
All checks passed.

Please shutdown Oracle instances running out of this ORACLE_HOME on the local system.
(Oracle Home = '/home/oracle/app/oracle/product/12.1.0/dbhome_1')

Is the local system ready for patching? [y|n]
y
User Responded with: Y
Backing up files...

Patching component oracle.rdbms, 12.1.0.2.0...

Verifying the update...
Patch 20830993 successfully applied
Log file location:/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/
20830993_Feb_25_2016_10_53_25/apply2016-02-25_10-53-25AM_1.log

OPatch succeeded.
```

d. Opatch ユーティリティを実行して、パッチが現在認識されていることを確認します。次の出力の最後に「Interim Patch」があることに注目してください。

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
   from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
```

```
Log file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_11-05-19AM_1.log
Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_11-0
5-19AM.txt

--------------------------------------------------------------------------------
Installed Top-level Products (1):
Oracle Database 12c                                                  12.1.0.2.0
There are 1 products installed in this Oracle Home.

Installed Products (135):

Assistant Common Files                                               12.1.0.2.0
Buildtools Common Files                                              12.1.0.2.0
Cluster Verification Utility Common Files                            12.1.0.2.0
Database Configuration and Upgrade Assistants                        12.1.0.2.0
Database Migration Assistant for Unicode                             12.1.0.2.0
Database SQL Scripts                                                 12.1.0.2.0
Database Workspace Manager                                           12.1.0.2.0
DB TOOLS Listener                                                    12.1.0.2.0
Deinstallation Tool                                                  12.1.0.2.0
Enterprise Edition Options                                           12.1.0.2.0
Expat libraries                                                       2.0.1.0.2
Generic Connectivity Common Files                                    12.1.0.2.0
Hadoopcore Component                                                 12.1.0.2.0
HAS Common Files                                                     12.1.0.2.0
HAS Files for DB                                                     12.1.0.2.0
Installation Common Files                                            12.1.0.2.0
Installation Plugin Files                                            12.1.0.2.0
Installer SDK Component                                              12.1.0.2.0
JAccelerator (COMPANION)                                             12.1.0.2.0
Java Development Kit                                                 1.6.0.75.0
LDAP Required Support Files                                          12.1.0.2.0
LAP SQL Scripts                                                      12.1.0.2.0
Oracle Advanced Security                                             12.1.0.2.0
Oracle Application Express                                           12.1.0.2.0
Oracle Bali Share                                                    11.1.1.6.0
Oracle Call Interface (OCI)                                          12.1.0.2.0
Oracle Clusterware RDBMS Files                                       12.1.0.2.0
Oracle Configuration Manager                                         10.3.8.1.1
Oracle Configuration Manager Client                                  10.3.2.1.0
Oracle Configuration Manager Deconfiguration                         10.3.1.0.0
Oracle Containers for Java                                           12.1.0.2.0
Oracle Context Companion                                             12.1.0.2.0
Oracle Core Required Support Files                                   12.1.0.2.0
Oracle Core Required Support Files for Core DB                       12.1.0.2.0
Oracle Core XML Development Kit                                      12.1.0.2.0
Oracle Data Mining RDBMS Files                                       12.1.0.2.0
Oracle Database 12c                                                  12.1.0.2.0
Oracle Database 12c                                                  12.1.0.2.0
Oracle Database 12c Multimedia Files                                 12.1.0.2.0
Oracle Database Deconfiguration                                      12.1.0.2.0
Oracle Database Gateway for ODBC                                     12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder           12.1.0.2.0
Oracle Database User Interface                                       11.0.0.0.0
Oracle Database Utilities                                            12.1.0.2.0
Oracle Database Vault option                                         12.1.0.2.0
Oracle DBCA Deconfiguration                                          12.1.0.2.0
Oracle Extended Windowing Toolkit                                    11.1.1.6.0
Oracle Globalization Support                                         12.1.0.2.0
Oracle Globalization Support                                         12.1.0.2.0
Oracle Globalization Support For Core                                12.1.0.2.0
Oracle Help for Java                                                 11.1.1.7.0
Oracle Help Share Library                                            11.1.1.7.0
```

```
Oracle Ice Browser                                                11.1.1.7.0
Oracle Internet Directory Client                                  12.1.0.2.0
Oracle Java Client                                                12.1.0.2.0
Oracle Java Layout Engine                                         11.0.0.0.0
Oracle JDBC Server Support Package                                12.1.0.2.0
Oracle JDBC/OCI Instant Client                                    12.1.0.2.0
Oracle JDBC/THIN Interfaces                                       12.1.0.2.0
Oracle JFC Extended Windowing Toolkit                             11.1.1.6.0
Oracle JVM                                                        12.1.0.2.0
Oracle JVM For Core                                               12.1.0.2.0
Oracle Label Security                                             12.1.0.2.0
Oracle LDAP administration                                        12.1.0.2.0
Oracle Locale Builder                                             12.1.0.2.0
Oracle Message Gateway Common Files                               12.1.0.2.0
Oracle Multimedia                                                 12.1.0.2.0
Oracle Multimedia Client Option                                   12.1.0.2.0
Oracle Multimedia Java Advanced Imaging                           12.1.0.2.0
Oracle Multimedia Locator                                         12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files             12.1.0.2.0
Oracle Multimedia Locator RDBMS Files                             12.1.0.2.0
Oracle Net                                                        12.1.0.2.0
Oracle Net Java Required Support Files                            12.1.0.2.0
Oracle Net Listener                                               12.1.0.2.0
Oracle Net Required Support Files                                 12.1.0.2.0
Oracle Net Services                                               12.1.0.2.0
Oracle Netca Client                                               12.1.0.2.0
Oracle Notification Service                                       12.1.0.2.0
Oracle Notification Service (eONS)                                12.1.0.2.0
Oracle Notification Service for Instant Client                    12.1.0.2.0
Oracle ODBC Driver                                                12.1.0.2.0
Oracle ODBC Driverfor Instant Client                              12.1.0.2.0
Oracle OLAP                                                       12.1.0.2.0
Oracle OLAP API                                                   12.1.0.2.0
Oracle OLAP RDBMS Files                                           12.1.0.2.0
Oracle One-Off Patch Installer                                    12.1.0.1.2
Oracle Partitioning                                               12.1.0.2.0
Oracle Programmer                                                 12.1.0.2.0
Oracle Quality of Service Management (Client)                     12.1.0.2.0
Oracle R Enterprise Server Files                                  12.1.0.2.0
Oracle RAC Deconfiguration                                        12.1.0.2.0
Oracle RAC Required Support Files-HAS                             12.1.0.2.0
Oracle Real Application Testing                                   12.1.0.2.0
Oracle Recovery Manager                                           12.1.0.2.0
Oracle Security Developer Tools                                   12.1.0.2.0
Oracle Spatial and Graph                                          12.1.0.2.0
Oracle SQL Developer                                              12.1.0.2.0
Oracle Starter Database                                           12.1.0.2.0
Oracle Text                                                       12.1.0.2.0
Oracle Text ATG Language Support Files                            12.1.0.2.0
Oracle Text for Core                                              12.1.0.2.0
Oracle Text Required Support Files                                12.1.0.2.0
Oracle Universal Connection Pool                                  12.1.0.2.0
Oracle Universal Installer                                        12.1.0.2.0
Oracle USM Deconfiguration                                        12.1.0.2.0
Oracle Wallet Manager                                             12.1.0.2.0
Oracle XML Development Kit                                        12.1.0.2.0
Oracle XML Query                                                  12.1.0.2.0
oracle.swd.oui.core.min                                           12.1.0.2.0
Parser Generator Required Support Files                           12.1.0.2.0
Perl Interpreter                                                  5.14.1.0.0
Perl Modules                                                      5.14.1.0.0
PL/SQL                                                            12.1.0.2.0
PL/SQL Embedded Gateway                                           12.1.0.2.0
```

```
Platform Required Support Files                                          12.1.0.2.0
Precompiler Common Files                                                 12.1.0.2.0
Precompiler Common Files for Core                                        12.1.0.2.0
Precompiler Required Support Files                                       12.1.0.2.0
Precompilers                                                             12.1.0.2.0
RDBMS Required Support Files                                             12.1.0.2.0
RDBMS Required Support Files for Instant Client                          12.1.0.2.0
RDBMS Required Support Files Runtime                                     12.1.0.2.0
Required Support Files                                                   12.1.0.2.0
Sample Schema Data                                                       12.1.0.2.0
Secure Socket Layer                                                      12.1.0.2.0
SQL*Plus                                                                 12.1.0.2.0
SQL*Plus Files for Instant Client                                        12.1.0.2.0
SQL*Plus Required Support Files                                          12.1.0.2.0
SQLJ Runtime                                                             12.1.0.2.0
SSL Required Support Files for InstantClient                             12.1.0.2.0
Tracle File Analyzer                                                     12.1.0.2.0
XDK Required Support Files                                               12.1.0.2.0
XML Parser for Java                                                      12.1.0.2.0
XML Parser for Oracle JVM                                                12.1.0.2.0
There are 135 products installed in this Oracle Home.

Interim patches (1) :

Patch  20830993      : applied on Thu Feb 25 10:53:50 PST 2016
Unique Patch ID:  18912657
Created on 13 May 2015, 00:37:38 hrs PST8PDT
   Bugs fixed:     20830993
Files Touched:
 /qksvc.o --> ORACLE_HOME/lib/libserver12.a
 ins_rdbms.mk --> ORACLE_HOME/rdbms/lib/ioracle
Patch Location in Inventory:
 /home/oracle/app/oracle/product/12.1.0/dbhome_1/inventory/oneoffs/20830993
Patch Location in Storage area:
 /home/oracle/app/oracle/product/12.1.0/dbhome_1/.patch_storage/20830993_May_13_2015_00_37_38
--------------------------------------------------------------------------------
```

プロセスを完了します。

「IoT FND データベースの設定」に進みます。

IoT FND データベースの設定

次の手順を実行して、IoT FND データベースを設定します。

- IoT FND データベースの設定の概要
- Oracle データベース環境変数の定義
- IoT FND Oracle データベース スクリプトのインストール
- IoT FND Oracle データベースの作成
- IoT FND Oracle データベースの起動

IoT FND データベースの設定の概要

IoT FND データベースを設定するには、次の手順を実行します。

1. Oracle データベース環境変数の定義。
2. IoT FND Oracle データベース スクリプトのインストール。

3. IoT FND Oracle データベースの作成。
4. IoT FND Oracle データベースの起動。

Oracle データベース環境変数の定義

IoT FND Oracle データベースをインストールする前に、**oracle** ユーザ アカウントに切り替え、次の Oracle データベースの環境変数を定義します。

表 6　Oracle データベースの環境変数

変数	説明
ORACLE_BASE	システムの Oracle ルート ディレクトリへのパスを定義します。次に例を示します。 `$ export ORACLE_BASE=/home/oracle/app/oracle` この変数を設定しないと、IoT FND のセットアップ スクリプトでエラーが表示されます。
ORACLE_HOME	IoT FND データベースの Oracle ホームへのパスを定義します。次に例を示します。 `$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1` (注) ORACLE_HOME 環境変数には、連続バックスラッシュを使用しないでください。
PATH	Oracle バイナリへのパスを定義します。次に例を示します。 `$ export PATH=$PATH:$ORACLE_HOME/bin`
LD_LIBRARY_PATH	ライブラリへのパスを定義します。次に例を示します。 `$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`

ORACLE_SID	Oracle システム ID (SID) を定義します。
	1 つのデータベース サーバだけを使用している場合、または HA 展開をインストールしている場合は、*プライマリ* データベース サーバでこの変数を **cgms** に設定します。
	`$ export ORACLE_SID=cgms`
	スタンバイ データベース サーバを展開している場合は、*スタンバイ* データベース サーバでこの変数を **cgms_s** に設定します。
	`$ export ORACLE_SID=cgms_s`
	この変数を設定しないと、IoT FND のセットアップ スクリプトでエラーが表示されます。

次の例に示すように、これらの変数を手動で設定できます。

シングルまたはプライマリ データベース サーバ	スタンバイ データベース サーバ

`$ su - oracle`
`$ export ORACLE_BASE=/home/oracle/app/oracle`
`$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1`
`$ export PATH=$PATH:$ORACLE_HOME/bin`
`$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
`$ export ORACLE_SID=cgms`
	`$ su - oracle`
	`$ export ORACLE_BASE=/home/oracle/app/oracle`
	`$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1`
	`$ export PATH=$PATH:$ORACLE_HOME/bin`
	`$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
	`$ export ORACLE_SID=cgms_s`

.bashrc ファイルを使用しても、これらの変数を定義できます。

IoT FND Oracle データベース スクリプトのインストール

IoT FND は、スクリプトおよび Oracle データベースのテンプレートとともにパッケージ化されています。

Oracle スクリプトを Oracle サーバにインストールするには、次の手順を実行します。

1. root ユーザとしてログインします。
2. IoT FND Oracle スクリプト RPM を Oracle サーバに安全にコピーします。

```
$ scp cgms-oracle-version_number.x86_64.rpm root@oracle-machine:~
$ rpm -ivh cgms-oracle-version_number.x86_64.rpm
```

3. cgms ディレクトリを作成し、ここにスクリプトとテンプレートをダウンロードします。

```
$ cd $ORACLE_BASE/app/oracle
$ mkdir cgms
$ cd cgms
$ cp -R /opt/cgms-oracle/scripts .
$ cp -R /opt/cgms-oracle/templates .
$ cp -R /opt/cgms-oracle/tools .
$ cd ..
$ chown -R oracle:dba cgms
```

IoT FND Oracle データベースの作成

シングル データベース サーバの展開で IoT FND Oracle データベースを作成するには、ユーザ *oracle* として setupCgmsDb.sh スクリプトを実行します。このスクリプトは、Oracle データベースを起動して、IoT FND データベースを作成します。

このスクリプトは、IoT FND がデータベースにアクセスするために使用するユーザ **cgms_dev** を作成します。このユーザ アカウントのデフォルト パスワードは **cgms123** です。

sys DBA アカウントのデフォルト パスワードは **cgmsDba123** です。

(注) デフォルト パスワードはすべて変更することを強く推奨します。encryption_util.sh スクリプトを使用する場合には、特殊文字(@、#、!、+ など)は使用しないでください。このスクリプトは特殊文字を暗号化することはできません。

(注) このスクリプトの実行には数分かかる場合があります。設定の進捗を確認するには、次のコマンドを実行します。

```
$ tail -f /tmp/cgmsdb_setup.log
```

```
$ su - oracle
$ export DISPLAY=localhost:0
$ cd $ORACLE_BASE/cgms/scripts
$ ./setupCgmsDb.sh
09-13-2012 10:38:07 PDT: INFO: ======== CGMS Database Setup Started ==========
09-13-2012 10:38:07 PDT: INFO: Log file: /tmp/cgmsdb_setup.log

Are you sure you want to setup CG-NMS database (y/n)? y

09-13-2012 10:38:08 PDT: INFO: User response: y
09-13-2012 10:38:08 PDT: INFO: CGMS database does not exist.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:38:14 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:38:18 PDT: INFO: User entered CG-NMS DB password.
09-13-2012 10:38:18 PDT: INFO: Stopping listener ...
09-13-2012 10:38:18 PDT: INFO: Listener already stopped.
09-13-2012 10:38:18 PDT: INFO: Deleting database files ...
09-13-2012 10:38:18 PDT: INFO: Creating listener ...
```

```
09-13-2012 10:38:19 PDT: INFO: Listener creation completed successfully.
09-13-2012 10:38:19 PDT: INFO: Configuring listener ...
09-13-2012 10:38:19 PDT: INFO: Listener successfully configured.
09-13-2012 10:38:19 PDT: INFO: Creating database.This may take a while.Please be patient ...
09-13-2012 10:42:55 PDT: INFO: Database creation completed successfully.
09-13-2012 10:42:55 PDT: INFO: Updating /etc/oratab ...
09-13-2012 10:42:55 PDT: INFO: /etc/oratab updated.
09-13-2012 10:42:55 PDT: INFO: Configuring database ...
09-13-2012 10:42:56 PDT: INFO: Starting listener ...
09-13-2012 10:42:56 PDT: INFO: Listener start completed successfully.
09-13-2012 10:42:56 PDT: INFO: Starting database configuration ...
09-13-2012 10:43:17 PDT: INFO: Database configuration completed successfully.
09-13-2012 10:43:17 PDT: INFO: Starting Oracle ...
09-13-2012 10:43:17 PDT: INFO: Starting Oracle in mount state ...
ORACLE instance started.

Total System Global Area 1.6836E+10 bytes
Fixed Size    2220032 bytes
Variable Size 8589934592 bytes
Database Buffers 8187281408 bytes
Redo Buffers   56487936 bytes
Database mounted.
09-13-2012 10:43:26 PDT: INFO: Opening database for read/write ...

Database altered.

09-13-2012 10:43:29 PDT: INFO: ========== CGMS Database Setup Completed Successfully ==========
```

IoT FND Oracle データベースの起動

IoT FND Oracle データベースを起動するには、次の手順を実行します。

1. 次のスクリプトを実行します。

```
$ su - oracle
$ cd $ORACLE_BASE/cgms/scripts
$ ./startOracle.sh
```

2. このスクリプトを実行して、ブートアップで IoT FND データベースを起動する cron ジョブを設定します。

```
./installOracleJob.sh
```

IoT FND データベースのその他のトピック

次の手順では、データベース管理について説明します。

- IoT FND Oracle データベースの停止
- IoT FND データベースの削除
- IoT FND データベースのアップグレード
- SYS DBA と IoT FND データベースのパスワードの変更
- IoT FND データベースのヘルパー スクリプト

IoT FND Oracle データベースの停止

通常、インストール手順で、Oracle データベースを停止する必要はありません。ただし、Oracle データベースの停止が必要になった場合には、scripts ディレクトリ内の停止スクリプトを使用します。

```
su - oracle
cd $ORACLE_BASE/cgms/scripts
./stopOracle.sh
...
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
...
```

IoT FND データベースの削除

注意: 次のスクリプトは破壊的です。このスクリプトは通常の操作では使用しないでください。

IoT FND データベースを削除するには、このスクリプトを実行します。

```
cd $ORACLE_BASE/cgms/scripts
./deleteCgmsDb.sh
```

IoT FND データベースのアップグレード

IoT FND データベースをアップグレードするには、次の手順を実行します。

1. データベース ファイル（合計 15 ファイル）を追加します。

   ```
   ALTER TABLESPACE USERS ADD DATAFILE '&oracle_base/oradata/&sid_caps/users<02 to 15>.dbf'
   SIZE 5M AUTOEXTEND ON;
   ```

これはシステムのスケーリングに必要です。

2. ブロック変更の追跡を有効化します（増分バックアップに必要）。

   ```
   ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
   '&oracle_base/oradata/&sid_caps/rman_change_track.f' REUSE;
   ```

3. 並列実行を無効にします。

   ```
   set parallel_max_servers = 0 scope=both
   ```

   注意: IoT FND の増分バックアップ スクリプトは、Oracle のブロック変更の追跡機能を有効にして、バックアップのパフォーマンスを向上させます。この機能を利用するには、IoT FND データベースを削除して、setupCgmsDb.sh スクリプトを実行してから、最初の増分バックアップを実行します。データの損失を回避するには、次のコマンドを実行します。

   ```
   sqlplus sys/password@cgms as sysdba
   ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
   '/home/oracle/app/oracle/oradata/CGMS/rman_change_track.f' REUSE;
   exit;
   ```

SYS DBA と IoT FND データベースのパスワードの変更

cgms_dba ユーザの IoT FND データベースのデフォルト パスワードを変更するには、次の手順を実行します。

1. IoT FND サーバで、setupCgms.sh スクリプトを実行し、cgms_dba ユーザのパスワードを変更します。

   注意: IoT FND データベースのパスワードと cgnms_dba ユーザのパスワードは一致している必要があります。一致していない場合、IoT FND はデータベースにアクセスできません。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
...
Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y
Enter database password:
Re-enter database password:
09-13-2012 17:15:31 PDT: INFO: Configuring database password.This may take a while.Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
...
```

setupCgms.sh スクリプトの実行については、「IoT FND のセットアップ」を参照してください。

2. Oracle サーバで、change_password.sh スクリプトを実行し、cgms_dba ユーザのパスワードを変更します。

```
$ ./change_password.sh
09-13-2012 10:48:32 PDT: INFO: ======== Database Password Util Started ==========
09-13-2012 10:48:32 PDT: INFO: Log file: /tmp/cgms_oracle.log

Are you sure you want to change CG-NMS database password (y/n)? y
09-13-2012 10:48:33 PDT: INFO: User response: y

Enter current password for SYS DBA:
Re-enter current password for SYS DBA:
09-13-2012 10:48:41 PDT: INFO: User entered current SYS DBA password.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:48:54 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:49:03 PDT: INFO: User entered CG-NMS DB password.
User altered.
...
```

(注) root としてこのスクリプトを使用すると、sys ユーザ（SYS DBA）のパスワードを変更することもできます。

3. IoT FND サーバで cgms_status.sh スクリプトを実行して、IoT FND と IoT FND データベース間の接続を確認します。

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

IoT FND データベースのヘルパー スクリプト

表 7 に、$ORACLE_BASE/cgms/scripts/ ディレクトリ内の使用可能な IoT FND データベースのヘルパー スクリプトを示します。

表 7　IoT FND データベースのヘルパー スクリプト

スクリプト	説明
change_password.sh	データベース管理と IoT FND データベース ユーザ アカウントのパスワードを変更するには、このスクリプトを使用します。IoT FND データベース ユーザ アカウントは、IoT FND がデータベースにアクセスするために使用されます。
backup_archive_log.sh	アーカイブ ログをバックアップするには、このスクリプトを使用します。
backupCgmsDb.sh	IoT FND データベースをバックアップするには、このスクリプトを使用します。このスクリプトは完全バックアップと増分バックアップをサポートします。
restoreCgmsDb.sh	バックアップから IoT FND データベースを復元するには、このスクリプトを使用します。

表 7　IoT FND データベースのヘルパー スクリプト（続き）

スクリプト	説明
setupCgmsDb.sh	IoT FND データベースを設定するには、このスクリプトを使用します。
startOracle.sh	IoT FND データベースを起動するには、このスクリプトを使用します。
stopOracle.sh	IoT FND データベースを停止するには、このスクリプトを使用します。
setupStandbyDb.sh	（IoT FND データベース HA のインストールのみ）スタンバイ データベース サーバを設定するには、このスクリプトを使用します。
setupHaForPrimary.sh	（IoT FND データベース HA のインストールのみ）プライマリ データベース サーバを設定するには、このスクリプトを使用します。
getHaStatus.sh	データベースが HA 用に設定されていることを確認するには、このスクリプトを実行します。

SSM のインストールと設定

ソフトウェア セキュリティ モジュール（SSM）は、ハードウェア セキュリティ モジュール（HSM）の低コストの代替策です。IoT FND は CSMP プロトコルを使用して、メーター、DA ゲートウェイ（IR500 デバイス）、および Range Extender と通信します。SSM は CiscoJ を使用して、CSMP メッセージの署名や確認などの暗号化サービス、およびを CSMP キーストア管理を提供します。SSM は連邦情報処理標準（FIPS）を順守しつつ、サービスを提供します。SSM は IoT FND アプリケーション サーバまたはその他のリモート サーバにインストールします。SSM のリモート コンピュータのインストールでは、IoT FND と安全に通信するため、HTTPS を使用します。

ここでは、SSM のインストールと設定について説明します。具体的な内容は次のとおりです。

- SSM サーバのインストールまたはアップグレード
- SSM サーバのアンインストール
- SSM と IoT FND の統合

SSM サーバをインストール、設定、起動し、SSM 用に IoT FND を設定すると、[Admin] > [Certificates] > [Certificate for CSMP] で CSMP の証明書を確認できます。

（注）ハードウェア セキュリティ モジュール（HSM）の詳細については、「HSM クライアントの設定」を参照してください。

はじめる前に

インストールが表 1 にリストしたハードウェアとソフトウェアの要件を満たしていることを確認します。

SSM サーバのインストールまたはアップグレード

SSM サーバをインストールするには、次の手順を実行します。

1. rpm スクリプト cgms-ssm-<version>-<release>.<architecture>.rpm を実行します。

```
[root@VMNMS demossm]# rpm -Uvh cgms-ssm-<version>.x86_64.rpm
Preparing...                ########################################### [100%]
   1:cgms-ssm               ########################################### [100%]
```

2. SSM に対する IoT FND の設定の詳細を取得します。SSM には次のデフォルトのクレデンシャルが同梱されています。
   - ssm_csmp_keystore パスワード：**ciscossm**
   - csmp のエイリアス名：**ssm_csmp**
   - キー パスワード：**ciscossm**
   - ssm_web_keystore パスワード：**ssmweb**

```
[root@VMNMS demossm]# cd /opt/cgms-ssm/bin/
[root@VMNMS bin]# ./ssm_setup.sh

Software Security Module Server
1.Generate a new keyalias with self signed certificate for CSMP
2.Generate a new keypair & certificate signing request for CSMP
3.Import a trusted certificate
4.Change CSMP keystore password
5.Print CG-NMS configuration for SSM
6.Change SSM server port
7.Change SSM-Web keystore password
Select available options.Press any other key to exit
Enter your choice :
```

3. プロンプトが表示されたら「5」を入力し、次を実行します。

```
Enter current ssm_csmp_keystore password :ciscossm
Enter alias name : ssm_csmp
Enter key password :ciscossm

security-module=ssm
ssm-host=<Replace with IPv4 address of SSM server>
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

4. この SSM サーバに接続するには、3. からの出力をコピーして cgms.properties ファイルに貼り付けます。

   (注) SSM サーバに接続するために使用する IoT FND のインターフェイスの IPv4 アドレスを含める必要があります。

5. (オプション) 以下を行うには、ssm_setup.sh スクリプトを実行します。

   - CSMP の新しいキー エイリアスと自己署名証明書を生成する
   - SSM キーストアのパスワードを変更する
   - SSM サーバ ポートを変更する
   - SSM-Web キーストアのパスワードを変更する

   (注) 上記のいずれかの操作を実行する場合、SSM セットアップ スクリプトを実行し、[Print CG-NMS configuration for SSM] を選択し、すべての詳細をコピーして cgms.properties ファイルに貼り付ける必要があります。

6. SSM サーバを起動します。

```
[root@VMNMS ~]# service ssm start
Starting Software Security Module Server:                  [  OK  ]
```

SSM ログ ファイルのモニタリング

SSM のログは、/opt/cgms-ssm/log/ssm.log でモニタできます。

レポート間隔のデフォルトのメトリックは、最小有効値の 900 秒 (15 分) です。サービスのメトリックのみが記録されます。レポートするメトリックがない場合、ログにメッセージは記録されません。

レポート間隔のメトリックは、/opt/cgms-ssm/conf/ssm.properties ファイルで [ssm-metrics-report-interval] フィールド (秒) を設定することで変更できます。

(注) IoT FND サーバを起動する前に、SSM サーバが起動され実行されている必要があります。

SSM サーバのアンインストール

ここでは、SSM サーバを完全にアンインストールする手順を示します。これには新規インストールの手順も含まれます。

(注) この手順はアップグレードには使用しないでください。SSM サーバのインストールまたはアップグレードで説明されている手順を使用します。

SSM サーバをアンインストールするには、次の手順を実行します。

1. SSM サーバを停止します。

   ```
   service ssm stop
   ```

2. /opt/cgms-ssm/conf ディレクトリとコンテンツを /opt/cgms-ssm の以外のディレクトリにコピーして移動します。
3. cgms ssm rpm をアンインストールします。

   ```
   rpm -e cgms-ssm
   ```

新規インストールのみ

4. 新しい SSM サーバをインストールします。
5. 2. で移動したコンテンツを /opt/cgms-ssm/conf ディレクトリにコピーして上書きします。

SSM と IoT FND の統合

(注) SSM に切り替える前に、SSM サーバをインストールして起動する必要があります。

CSMP ベースのメッセージングに、ハードウェア セキュリティ モジュール(HSM)の使用から SSM の使用に切り替えるには、次の手順を実行します。

1. IoT FND を停止します。

   ```
   service cgms stop
   ```

2. SSM サーバで ssm_setup.sh スクリプトを実行します。
3. オプション 3 を選択し、IoT FND SSM 設定を印刷します。
4. 詳細を cgms.properties にコピー アンド ペーストして、SSM サーバに接続します。

   例

   ```
   security-module=ssm
   ssm-host=127.107.155.85
   ssm-port=8445
   ssm-keystore-alias=ssm_csmp
   ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
   ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
   ```

5. HSM を設定するには、cgms.properties ファイルで次のプロパティを指定します(「HSM クライアントの設定」も参照)。

   ```
   security-module=ssm/hsm (required; hsm : Hardware Security Module default.)
   hsm-keystore-name=testGroup1 (optional; hsm partition name; testGroup1 default)
   hsm-keystore-password=TestPart1 (optional; encrypted hsm partition password; TestPart1 default)
   ```

6. SSM が起動して動作しており、接続できることを確認します。
7. IoT FNDを起動します。

IoT FND のインストールおよびセットアップ

次の手順を実行して、IoT FND のインストールを完了します。

- インストールと設定の概要
- IoT FND のインストール
- 証明書の生成およびインストール
- IoT FND のセットアップ
- IoT FND の起動
- IoT FND ステータスのチェック
- IoT FND データベース移行スクリプトの実行
- IoT FND Web GUI へのアクセス

はじめる前に

IoT FND をインストールするには、最初に IoT FND のインストール RPM を取得します。

`cgms-version_number.x86_64.rpm`

(注) /etc/hosts ファイルと /etc/resolv.conf ファイルが IoT FND サーバで正しく設定されていることを確認します。

インストールと設定の概要

ここでは、2 つのタイプの IoT FND のインストールの概要を提供します。

- シングルサーバの展開
- クラスタ展開(HA)

シングルサーバの展開

シングルサーバの展開に IoT FND をインストールして設定するには、次の手順を実行します。

1. IoT FND をホストする RHEL サーバにログインします。
2. IoT FND のインストール。
3. IoT FND のセットアップ。
4. IoT FND データベース移行スクリプトの実行。
5. IoT FND ステータスのチェック。
6. IoT FND Web GUI へのアクセス

クラスタ展開(HA)

HA 展開に IoT FND をインストールして設定するには、「シングルサーバの展開」のステップを繰り返します。ただし、IoT FND データベースの移行スクリプトは 1 回だけ実行します。

IoT FND のインストール

IoT FND アプリケーションをインストールするには、次の手順を実行します。

1. IoT FND インストール RPM を実行します。

```
$ rpm -ivh cgms-version.x86_64.rpm
```

2. インストールを確認し、RPM バージョンを確認します。

```
$ rpm -qa | grep -i cgms
cgms-1.0
```

IoT FND のセットアップ

IoT FND を設定するには、setupCgms.sh スクリプトを実行します。

(注) IoT FND サーバ クラスタを展開している場合、クラスタ内のすべてのノードで setupCgms.sh スクリプトを実行する必要があります。

注意：IoT FND 証明書はデータベースのデータを暗号化します。setupCgms.sh スクリプトは、データベースの移行を実行します。これには、キーストア内の IoT FND 証明書へのアクセスが必要です。setupCgms.sh を実行する前に証明書を設定する必要があります。データベースを移行し、証明書にアクセスできない場合、スクリプトはエラーになります(「証明書の生成およびインストール」を参照)。

注意：setupCgms.sh スクリプトの実行時に、入力したデータベース パスワードが有効であることを確認します。無効なパスワードを複数回入力すると、Oracle によってユーザ アカウントがロックされる場合があります。アカウントのロック解除はデータベース サーバでできます。パスワードのロック解除の詳細については、「IoT FND データベース パスワードのロック解除」を参照してください。

この例では、setupCgms.sh スクリプトを使用して、1 つのデータベースを使用するシングルサーバの IoT FND システムを設定します。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms

Do you wish to configure another database server for this CG-NMS ? (y/n)? n

09-13-2012 17:11:18 PDT: INFO: User response: n
09-13-2012 17:11:18 PDT: INFO: Configuring database settings.This may take a while.Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y
```

```
09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password.This may take a while.Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n
09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

setupCgms.sh スクリプトでは、これらの設定を行うことができます。

- データベース設定の構成
- データベース HA の構成
- IoT FND データベース パスワードの設定
- キーストア パスワードの設定
- Web root ユーザ パスワードの設定
- FTPS 設定の構成

データベース設定の構成

データベース設定を構成するため、setupCgms.sh スクリプトによって次の情報の入力が求められます。

- プライマリ IoT FND データベース サーバの IP アドレス
- IoT FND データベース サーバのポート番号

  デフォルトのポート番号(1522)を受け入れるには、Enter キーを押します。
- データベース システム ID(SID)。これはプライマリ データベース サーバの cgms です。

  デフォルトの SID(cgms)を受け入れるには、Enter キーを押します。この SID はサーバをプライマリ データベース サーバと見なします。

```
Do you want to change the database settings (y/n)? y
09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

データベース HA の構成

スタンバイ データベース設定を構成するため、setupCgms.sh スクリプトによって次の情報の入力が求められます。

- スタンバイ IoT FND データベース サーバの IP アドレス
- スタンバイ IoT FND データベース サーバのポート番号

  1522 と入力します。
- データベース システム ID（SID）。これはプライマリ データベース サーバの cgms です。

  cgms_s を入力します。この SID はサーバをスタンバイ データベース サーバと見なします。

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings.This may take a while.Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.
```

データベース HA の設定については、「HA 用の IoT FND データベースの設定」を参照してください。

IoT FND データベース パスワードの設定

IoT FND データベースのパスワードを変更するよう求められたら、データベース サーバで cgms_dba ユーザ アカウントのパスワードを入力します。デフォルトのパスワードを使用している場合、データベース パスワードをここで変更しないでください。

```
Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password.This may take a while.Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
```

キーストア パスワードの設定

キーストア パスワードを設定します。

```
Do you want to change the keystore password (y/n)? y
09-13-2012 10:21:52 PDT: INFO: User response: y

Enter keystore password: keystore_password
Re-enter keystore password: keystore_password

09-13-2012 10:21:59 PDT: INFO: Configuring keystore password.This may take a while.Please wait
...09-13-2012 10:22:00 PDT: INFO: Keystore password configured.
```

Web root ユーザ パスワードの設定

ブラウザベースの IoT FND インターフェイスへのアクセスを可能にする root ユーザ アカウントのパスワードを変更するには、**y** を入力し、パスワードを入力します。

```
Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n
```

FTPS 設定の構成

クラスタを展開している場合は、ログのダウンロードに必要な FTPS 設定を提供します。FTPS は、クラスタ ノード間で安全にファイルを転送します。FTPS 設定が構成されていない場合、現在ログインしている IoT FND ノードからログだけをダウンロードできます。

```
Do you want to change the FTP settings (y/n)? y
09-13-2012 17:16:45 PDT: INFO: User response: y

Enter FTP user password:
Re-enter FTP user password:

09-13-2012 17:16:49 PDT: INFO: Configuring FTP settings.This may take a while.Please wait ...
09-13-2012 17:16:57 PDT: INFO: FTP settings configuration completed successfully
```

IoT FND ステータスのチェック

IoT FND を起動する前に、このコマンドを実行して IoT FND データベースへの接続を確認します。

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

このコマンドにより、IoT FND データベースの IP アドレスまたはホスト名およびステータスが提供され、IoT FND データベースへの接続も確認されます。接続が確認されない場合、IoT FND を起動することはできません。

IoT FND データベース移行スクリプトの実行

IoT FND はデータベースのダンプと復元を行わずに、IoT FND データベースをすばやく移行できる特別なデータベースの移行システムを使用しています。データベースを移行するたび、IoT FND がすでに実行された移行のレコードを維持できるように、IoT FND データベースの一部のテーブルが作成または変更されます。

最初に IoT FND を起動する前に、データベース移行スクリプトを実行して、データベースの IoT FND テーブルを設定します。

```
# cd /opt/cgms/bin
# ./db-migrate
```

(注)IoT FND を初めて起動する前にこのスクリプトを実行すると、数分かかります。IoT FND の新しいバージョンへのアップグレード後にこのスクリプトを実行すると、IoT FND データベースのデータ量によってはさらに時間がかかります。

(注)IoT FND サーバ クラスタを展開している場合、1 つのクラスタ ノードでのみ db-migrate スクリプトを実行します。

db-migrate コマンドでは、データベース パスワードが要求されます。デフォルト パスワードは **cgms123** です。

注意:db-migrate スクリプトの実行時に入力したパスワードが正しいことを確認します。間違ったパスワードを複数回入力すると、Oracle によってユーザ アカウントがロックされる場合があります。この場合、データベース サーバでアカウントのロック解除をする必要があります。パスワードのロック解除の詳細については、「IoT FND データベース パスワードのロック解除」を参照してください。

IoT FND Web GUI へのアクセス

IoT FND にはその Web GUI の自己署名証明書が含まれています。IoT FND GUI にアクセスするには、ブラウザにセキュリティ例外を追加する必要があります。IoT FND を起動すると、その Web GUI にアクセスできます。

https://*nms_machine_IP_address*/

デフォルトの初期ユーザ名は root で、パスワードは **root123** です。

セットアップ スクリプトの実行時にパスワードを変更した場合を除き、IoT FND はデフォルトのパスワード **root123** を使用します。

セットアップ スクリプトの詳細については、「IoT FND のセットアップ」を参照してください。

(注) IoT FND にハードウェア セキュリティ モジュール(HSM)が含まれている場合、Firefox ブラウザは IoT FND に接続しません。この問題に対処するには、Firefox の [Preferences] を開き、[Advanced] に移動して [Encryption] タブをクリックします。[Protocols] の下の [Use TLS 1.0] チェック ボックスをオフにします。IoT FND に再接続し、ページが正常にロードされたことを確認します。

HTTPS 接続

IoT FND は TLSv1.2 ベースの HTTPS 接続のみを受け入れます。IoT FND GUI にアクセスするには、TLSv1.2 プロトコルを有効にして、IoT FND との HTTPS 接続を確立する必要があります。

(注) IoT FND リリース 2.1.1-54 以降では、TLSv1.0 または TLSv1.1 ベースの接続をサポートしていません。

初めてのログイン

初めて IoT FND にログインすると、パスワードの変更を求めるポップアップ ウィンドウ(図 1)が表示されます。

図 1　　IoT FND の初期パスワードの変更

(注) IoT FND では、最大 32 文字のパスワード長をサポートしています。

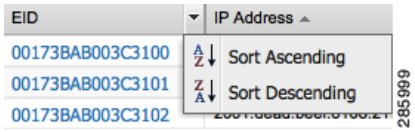
タイム ゾーンの設定

タイム ゾーンを設定するには、以下のステップに従います。

1. [username] ドロップダウン メニュー(右上)から、[Time Zone] を選択します。
2. 時間帯を選択します。
3. [Update Time Zone] をクリックします。
4. [OK] をクリックします。

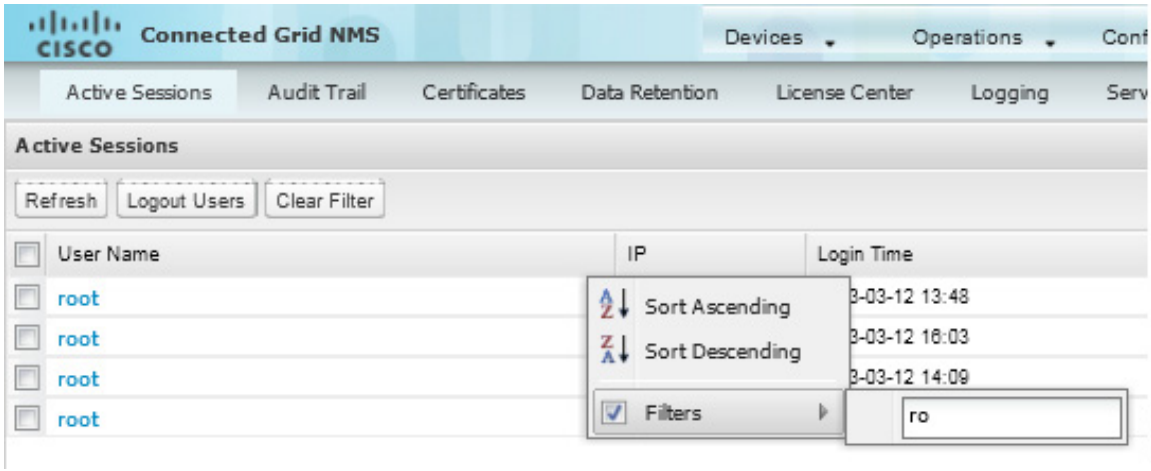
列のソート順序の変更

IoT FND が列見出しのあるリストを表示するすべてのページで、この例のように、[Sort] ドロップダウン メニューを使用して、列のソート順序を変更できます。

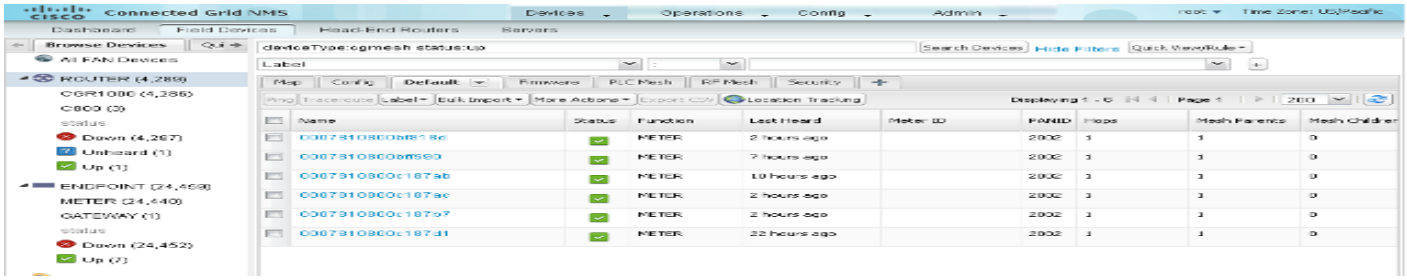


リストのフィルタリング

IoT FND では、フィルタを定義できます。次の例では、[User Name] 列のドロップダウン メニューの [Filters] フィールドに「ro」を入力すると、「ro」から始まるユーザ名を持つユーザのアクティブなセッションがリストされます。フィルタをリセットするには、[Clear Filter] ボタンをクリックします。

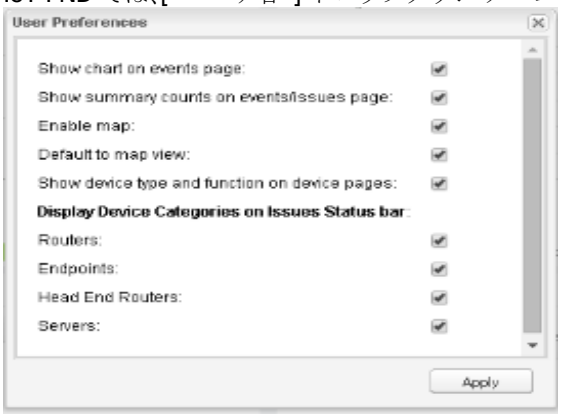


次の例では、[Search Devices] フィールドに検索文字列「**deviceType:cgmesh status:up**」を入力することで、Up ステータスのメッシュ エンドポイント デバイスをリストします。



ユーザ プリファレンスの設定

IoT FND では、[<ユーザ名>] ドロップダウン メニュー（右上）から、次の設定を設定することができます。



- [Events] ページ（[Operations] > [Events]）でのイベント チャートの表示を有効にする。
- [Events] ページ（[Operations] > [Events]）でのイベント数の表示を有効にし、[Issues] ページ（[Operations] > [Issues]）での問題の数の表示を有効にする。イベントまたは問題のステータスの横の左側ペインに数が表示されます。
- [Map View] ペイン（[Devices] > [Field Devices]）の表示を有効にする。
- [Map View]（[Devices] > [Field Devices]）へのデフォルトの表示を設定する。
- [Issues] ステータス バーに表示する問題のデバイス タイプを設定する。

ログアウト

IoT FND のログアウトをするには、[<ユーザ名>] ドロップダウン メニュー（右上）の [Log Out] をクリックします。

IoT FND CLI

このセクションでは、IoT FND を管理するための次のコマンドを紹介します。

- IoT FND の起動
- IoT FND ステータスのチェック
- IoT FNDの停止
- IoT FND ログ ファイルの場所
- IoT FND ヘルパー スクリプト
- IoT FND のアップグレード
- IoT FND のアンインストール

IoT FND の起動

IoT FND を起動するには、このコマンドを実行します。

```
service cgms start
```

IoT FND がブート時に自動的に動作するように設定するには、このコマンドを実行します。

```
chkconfig cgms on
```

IoT FND ステータスのチェック

IoT FND のステータスを確認するには、このコマンドを実行します。

```
service cgms status
```

IoT FNDの停止

IoT FND を停止するには、このコマンドを実行します。

```
service cgms stop
```

(注)アプリケーションが停止するには、通常、約 10 秒かかります。Java プロセスが実行されていないことを確認するには、**ps | grep java** を実行します。

IoT FND ログ ファイルの場所

IoT FND ログ ファイル(server.log)は /opt/cgms/server/cgms/log ディレクトリにあります。

IoT FND ヘルパー スクリプト

表 8 で、/opt/cgms/bin/ ディレクトリ内の IoT FND ヘルパー スクリプトについて説明します。

表 8　　IoT FND ヘルパー スクリプト

スクリプト	説明
deinstall_cgms_watchdog.sh	ウォッチドッグ スクリプトをアンインストールします。
install_cgms_watchdog.sh	ウォッチドッグ スクリプトをインストールします。
mcast_test.sh	クラスタ メンバー間の通信をテストします。
password_admin.sh	IoT FND へのアクセスに使用するユーザ パスワードを変更またはリセットします。
print_cluster_view.sh	クラスタ メンバーを印刷します。

IoT FND のアップグレード

(注)通常のアップグレード時には、データベースを停止する必要はありません。すべてのアップグレードはインプレースです。

(注)カスタム セキュリティ証明書を使用した仮想 IoT FND のインストールについては、このアップグレードを実行する前に「カスタム証明書の管理」を参照してください。

注意:次の手順を順に実行します。

IoT FND アップグレードするには、次の手順を実行します。

1. 新しい IoT FND RPM を取得します。
2. IoT FND を停止します。

   ```
   service cgms stop
   ```

   (注)アプリケーションが停止するには、通常、約 10 秒かかります。Java プロセスが実行されていないことを確認するには、**ps | grep java** を実行します。
3. IoT FND RPM をアップグレードします。

   ```
   rpm -Uvh new_cgms_rpm_filename
   ```

   (注)これらのファイルは、/opt/cgms 内のファイルを上書きします。

4. データベースの移行を実行し、/opt/cgms ディレクトリからデータベースをアップグレードします。

```
cd /opt/cgms
bin/db-migrate
```

(注) db-migrate スクリプトは、アップグレードが終了するたびに実行する必要があります。

5. プロンプトが表示されたら、データベースのパスワードを入力します。デフォルト パスワードは **cgms123** です。

6. IoT FND を起動します。

```
# service cgms start
```

RHEL GUI を使用しても、IoT FND サービスを開始できます([Admin] > [Server Settings] > [Services])。詳細については、RHEL のマニュアルを参照してください。

IoT FND のアンインストール

(注) これは、すべての IoT FND のローカル インストールの設定とインストール ファイル(証明書を含むキーストアなど)を削除します。

ヒント:IoT FND を再インストールする予定がある場合は、現在のキーストアと証明書ファイルをコピーして、インストール パッケージに含まれるキーストアと証明書ファイルを上書きするのに使用します。

IoT FND アプリケーションを削除するには、次のコマンドを実行します。

```
# rpm -e cgms
# rm -rf /opt/cgms
```

IoT FND データベースのクリーンアップ

IoT FND データベースをクリーンアップするには、次の手順を実行します。

1. (HA データベース設定)オブザーバ サーバを停止します。

2. (HA データベース設定)$ORACLE_BASE/cgms/scripts/ha/deleteStandbyDb.sh スクリプトを実行して、スタンバイ データベースを削除します。

3. (HA データベース設定)$ORACLE_BASE/cgms/scripts/ha/deletePrimaryDbHa.sh スクリプトを実行して、プライマリ データベースから HA 設定を削除します。

4. $ORACLE_BASE/cgms/scripts/deleteCgmsDb.sh スクリプトを実行して、プライマリ データベースを削除します。

IoT FND TPS プロキシのインストールと設定

オプション TPS プロキシを初めて使用するのは、通常、IoT FND が処理する ZTD の部分を初期化するインバウンド要求を CGR が送信するときです。IoT FND はファイアウォールの背後で稼働しており、パブリックで到達可能な IP アドレスがありません。FAR(CGR と ISR)が IoT FND に初めてコンタクトするときに、IoT FND は FAR に TPS プロキシを使用することを求めます。このサーバは FAR が IoT FND アプリケーション サーバにコンタクトして、トンネル プロビジョニングを要求できるようにします(「トンネルのプロビジョニングの管理」を参照)。

TPS プロキシには独自の GUI はありません。HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、**cgnms.properties** ファイルと **tpsproxy.properties-template** ファイルでプロパティを編集する必要があります。

トンネルをプロビジョニングすると、FAR は TPS プロキシを使用せずに IoT FND に直接コンタクトすることができます。IoT FND にプロキシの証明書から正確な証明書の件名が通知され、TPS プロキシからの HTTPS インバウンド要求が認証されます。

TPS プロキシの設定

cgms-tpsproxy RPM パッケージ Java アプリケーションを、ファイアウォールの外側の IoT FND のステートレス拡張として機能するように、別の（TPS プロキシ）サーバにインストールします。TPS プロキシは Red Hat Enterprise Linux（RHEL）サーバ（表 1 の TPS プロキシのシステム要件を参照）が可能です。cgnms-tpsproxy アプリケーションはサーバでデーモンとして実行され、次の設定パラメータを必要とします。

- IoT FND サーバの URL（インバウンド要求を転送するため）。
- アウトバウンド要求を転送するためのホワイトリスト（認定リスト）の一部としての IoT FND サーバの IP アドレス。

TPS プロキシをインストールする前に、TPS プロキシのインストール パッケージを取得します。

`cgms-tpsproxy-version_number.x86_64.rpm`

プロキシサーバの設定を構成するには、次の手順を実行します。

1. TPS プロキシとして使用するように RHEL サーバを設定します。
2. この RHEL サーバをファイアウォールの外側で到達できるように接続します。
3. テンプレート ファイルを使用して TPS プロキシを設定します。

```
ssh root@tps_proxy_server
cd /opt/cgms-tpsproxy/conf
cp tpsproxy.properties-template tpsproxy.properties
```

(注) IoT FND TPS プロキシの登録時に encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。

4. tpsproxy.properties ファイルを編集して、IoT FND アプリケーション サーバのインバウンド アドレスとアウトバウンド アドレスを定義する次の行を追加します。

```
[root@cgr-centos57 conf]# cat tpsproxy.properties-template
inbound-proxy-destination=https://nms_domain_name:9120
outbound-proxy-allowed-addresses=nms_ip_address
cgms-keystore-password-hidden=<obfuscated password>
```

(注) HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを編集する必要があります。

TPS プロキシ ファイアウォールの設定

TPS プロキシ ファイアウォールを設定するには、次の手順を実行します。

- ポート 9120 で TPS プロキシから IoT FND サーバへの HTTPS 接続を許可するファイアウォール ルールを設定します（HTTPS インバウンド要求）。
- ポート 9122 で IoT FND サーバから TPS プロキシへの HTTPS 接続を許可するファイアウォール ルールを設定します（HTTPS アウトバウンド要求）。

IoT FND TPS プロキシの登録

TPS プロキシの登録プロセスは、IoT FND の登録プロセスと同じです。IoT FND アプリケーション サーバの証明書に署名する認証局（CA）は、TPS プロキシの証明書にも署名する必要があります。TPS プロキシの証明書は Java キーストアに保存され、IoT FND 証明書に似ています。

登録プロセスについては、次のシナリオを検討してください。

- 新規インストール
  - キーストアのパスワードがデフォルト パスワードと同じ場合は、デフォルト パスワードを変更します。

    (注) デフォルト パスワードはすべて変更することを強く推奨します。encryption_util.sh スクリプトは特殊文字を暗号化できないため、@、#、!、+ などの特殊文字は使用しないでください。

  - キーストア パスワードがデフォルト パスワードとは異なっている場合、encryption_util.sh スクリプトを実行して、暗号化されたパスワードを properties ファイルにコピーします。

    (注) encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。

- アップグレード

  デフォルト パスワードまたはカスタム パスワードを使用しているかどうかに関わらず、アップグレード プロセスでは /opt/cgms-tpsproxy/conf/tpsproxy.properties ファイルのパスワードが暗号化されます。

IoT FND の登録の詳細については、「*Generating and Exporting Certificates*」を参照してください。

端末 TPS プロキシを登録するには、次の手順を実行します。

1. **cgms_keystore** ファイルを作成します。
2. このファイルに証明書を追加します。
3. **/opt/cgms-tpsproxy/conf** ディレクトリにファイルをコピーします。

TPS プロキシを使用するための IoT FND の設定

HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを編集する必要があります。TPS プロキシは、すべてのインバウンドおよびアウトバウンド要求をログに記録します。

(注) cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを設定しないと、IoT FND は TPS プロキシを認識せず、転送された要求をドロップし、不明なデバイスからの要求と見なします。

(注) 次の例では、必須の値でない変数を使用しています。これらは例としてのみ提示しています。

TPS プロキシを使用するように IoT FND を設定するには、次の手順を実行します。

1. IoT FND サーバへの SSH 接続を開きます。

   ```
   ssh root@nms_machine
   cd /opt/cgms/server/cgms/conf/
   ```

   (注) IoT FND TPS プロキシの登録時に encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。

2. **cgdm tpsproxy** ファイルを編集して、cgdm-tpsproxy-subject プロパティに TPS プロキシの IP アドレス、ドメイン名、ユーザの情報カテゴリを特定する行を追加します。

   (注) cgdm-tpsproxy-subject プロパティは、インストールされた TPS プロキシの証明書と一致する必要があります。

   ```
   cgdm-tpsproxy-addr=proxy_server_IP_address
   cgdm-tpsproxy-subject=CN="common_name", OU="organizational_unit", O="organization", L="location",
   ST="state", C="country"
   ```

   (注) カンマ区切りの文字列を引用符で囲みます。

IoT FND TPS プロキシの起動

インストール、設定、登録を行ったら、TPS プロキシを起動します。

TPS プロキシを起動するには、起動スクリプトを実行します。

```
service tpsproxy start
```

TPS プロキシのログ ファイルは次の場所にあります。

```
/opt/cgms-tpsproxy/log/tpsproxy.log
```

(注)詳細については、「TPS プロキシの検証」を参照してください。

TPS プロキシの検証

TPS プロキシはインバウンドおよびアウトバウンドのすべての HTTPS 要求を、/opt/cgms-tpsproxy/log/tpsproxy.log にある TPS ログ ファイルに記録します。

TPS プロキシの tpsproxy.log ファイルの次のエントリは、CGR のインバウンド要求を定義します。

```
73: cgr-centos57: May 21 2014 01:05:20.513 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][eid=CGR1240/K9+JAF1732ARCJ][ip=192.168.201.5][sev=INFO][tid=qtp46675819-
29]: Inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

TPS プロキシの tpsproxy.log ファイルのこのメッセージ エントリは、TPS が正常にメッセージを IoT FND に転送したことを示します。

```
74: cgr-centos57: May 21 2014 01:05:20.564 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][sev=INFO][tid=com.cisco.cgms.tpsproxy.TpsProxyServlet-49dc423f-22]:
Completed inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

IoT FND サーバのログ ファイル内の次のエントリは、TPS プロキシを特定します。

```
Request came from proxy
Using forwarded client subject (CN=cg-cgr-1, SERIALNUMBER=PID:CGR1240/K9 SN:JSJ15220047) for
authentication
```

TPS プロキシの tpsproxy.log ファイルの次のエントリは、アウトバウンド要求を定義します。

```
%CGMS-6-UNSPECIFIED: %[ch=TpsProxyOutboundHandler][ip=192.168.205.5][sev=INFO][tid=qtp257798932-15]:
Outbound proxy request from [192.168.205.5] to [192.168.201.5:8443]
```

IoT FND サーバのログ ファイル内の次のエントリは、HTTPS 接続を特定します。

```
Using proxy at 192.168.201.6:9122 to send to https://192.168.201.4:8443/cgdm/mgmt commands:
```

Dual-PHY 用の IoT FND の設定

Dual-PHY CGR では、デバイス追加ファイルで Dual-PHY パラメータ(表 13 を参照)を設定して、すべての Dual-PHY WPAN モジュール(マスターおよびスレーブ)を設定する必要があります。適切なデバイス追加ファイルで設定するパラメータは、**masterWpanInterface** と **slaveWpanInterface** です。スレーブ Dual-PHY WPAN デバイスでは、**slave-mode** パラメータも設定する必要があります。

(注)Dual-PHY CGR の設定情報については、『*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。

例

次の例は、設定のプッシュ時にどの WPAN デバイスをマスター インターフェイスとスレーブ インターフェイスとして割り当てるかを IoT FND に指示します。

```
deviceType,eid,ip,meshPrefixConfig,meshPrefixLengthConfig,meshPanidConfig,meshAddressConfig,
dhcpV4LoopbackLink,dhcpV4TunnelLink,dhcpV6LoopbackLink,dhcpV6TunnelLink,tunnelSrcInterface1,
tunnelHerEid,adminUsername,adminPassword,certIssuerCommonName,ipsecTunnelDestAddr1,
masterWpanInterface,slaveWpanInterface,lat,lng
cgr1000,CGR1240/K9+JAF1741BFQS,2.2.56.253,2319:EXTRA:BEEF:CAFE::,64,1233,
2319:EXTRA:BEEF:CAFE::,20.211.0.1,20.211.0.1,2001:420:7bf:7e8::1,
2001:420:7bf:7e8::1,GigabitEthernet2/1,cg-isr900,cg-nms-administrator,
0ERIF+cKsLwyT0YTFd0k+NpVAAPxcIvFfoX1sogAXVkSOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+
pEQ1aIQvIGuIas9wp9MKUARYpNErXRiHEnpeH044Rfa4uSgsWXEyrVNxHyuvSefB5j6H0uA7tIQwEHDXOiq
/d0yxvfd4IYos7NzPXlJNiR+Cp6bwx7dG+d9Jo+JuNxLXpi8Fo5n88usjMoXPNbyrqvgn7SS4f+VYgXx1iyDNP0k
+7OEE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMijPstDBXpFv8dqtA0xDGKuaRg
==,cenbursaca-cenbu-sub-ca,2.2.55.198,Wpan3/1,Wpan5/1,41.413324,-120.920315
```

以下は、CGR WPAN モジュールでのマスター/スレーブ インターフェイスを設定するための標準的なテンプレートです。

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154  panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
ieee154 ssid cisco_muruga_dual
ieee154 txpower 21
slave-mode 3
rpl dag-lifetime 240
rpl dio-min 21
rpl version-incr-time 240
authentication host-mode multi-auth
authentication port-control auto
ipv6 dhcp relay destination global  2001:420:7BF:5F::705
dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
end
```

Dual-PHY デバイスのメッシュ セキュリティ キー

(注) スレーブ WPAN デバイスにはメッシュ セキュリティ キーを設定しないでください。

IoT FND でマスター/スレーブ モードが正しく設定されていると、IoT FND は自動的にマスター WPAN を検出し、そのメッシュ セキュリティ キーを設定します。既存の CGR を設定し、別の WPAN インターフェイスを追加すると、すべてのメッシュ セキュリティ キーが両方のインターフェイスから削除され、IoT FND によりマスター/スレーブ モードが設定されます。CGR が接続されると、すべてのメーターが再認証を経由します。

次のコマンドを使用して、メッシュ キーを削除できます。

```
mesh-security expire mesh-key interface wpan <slot>/<slot number>
```

設定例

次の例では、現在の Dual-PHY WPAN デバイスの RPL スロット ツリー、RPL スロット テーブル、RPL IP ルート情報テーブル、スロット 4/1 と 3/1 の設定情報を取得します。

```
cisco-NXT-FAR5#show wpan 4/1 rpl stree

---------------------------- WPAN RPL SLOT TREE [4] -----------------------------

  [2001:RTE:RTE:64::4]
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800    // SY RF nodes
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00    // CY PLC nodes
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07

RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)


cisco-NXT-FAR5#ping 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms

cisco-NXT-FAR5#ping 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-NXT-FAR5#

cisco-NXT-FAR5#show wpan 4/1 rpl stable

------------------------------ WPAN RPL ROUTE SLOT TABLE [4] ------------------------------
NODE_IPADDR                    NEXTHOP_IP                    SSLOT LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800        2001:RTE:RTE:64::4                       3      17:49:12
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        2001:RTE:RTE:64::4                       3      18:14:05
2001:RTE:RTE:64:207:8108:3C:1802        2001:RTE:RTE:64::4                       3      18:14:37
2001:RTE:RTE:64:207:8108:3C:1803        2001:RTE:RTE:64::4                       3      17:56:56
2001:RTE:RTE:64:207:8108:3C:1804        2001:RTE:RTE:64::4                       3      17:48:53
2001:RTE:RTE:64:207:8108:3C:1805        2001:RTE:RTE:64::4                       3      17:47:52
2001:RTE:RTE:64:207:8108:3C:1806        2001:RTE:RTE:64::4                       3      17:49:54
2001:RTE:RTE:64:207:8108:3C:1807        2001:RTE:RTE:64::4                       3      17:46:38
2001:RTE:RTE:64:207:8108:3C:1808        2001:RTE:RTE:64::4                       3      18:22:01
2001:RTE:RTE:64:207:8108:3C:1809        2001:RTE:RTE:64::4                       3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180A        2001:RTE:RTE:64::4                       3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180B        2001:RTE:RTE:64::4                       3      18:24:00
2001:RTE:RTE:64:207:8108:3C:1A00        2001:RTE:RTE:64:207:8108:3C:1801         3      17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01        2001:RTE:RTE:64:207:8108:3C:180B         3      18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02        2001:RTE:RTE:64:207:8108:3C:180B         3      18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03        2001:RTE:RTE:64:207:8108:3C:1805         3      18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04        2001:RTE:RTE:64:207:8108:3C:180B         3      17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05        2001:RTE:RTE:64:207:8108:3C:180B         3      18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06        2001:RTE:RTE:64:207:8108:3C:180B         3      18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07        2001:RTE:RTE:64:207:8108:3C:1805         3      17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08        2001:RTE:RTE:64:207:8108:3C:180B         3      18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09        2001:RTE:RTE:64:207:8108:3C:180B         3      18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A        2001:RTE:RTE:64:207:8108:3C:180B         3      18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B        2001:RTE:RTE:64:207:8108:3C:180B         3      18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02        2001:RTE:RTE:64:207:8108:3C:1A06         3      18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04        2001:RTE:RTE:64:207:8108:3C:1A06         3      18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:10:02
2001:RTE:RTE:64:207:8108:3C:1C06        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00        2001:RTE:RTE:64::4                       4      18:21:40

// CY PLC nodes
2001:RTE:RTE:64:217:3BCD:26:4E01        2001:RTE:RTE:64::4                       4      17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02        2001:RTE:RTE:64::4                       4      18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03        2001:RTE:RTE:64::4                       4      17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04        2001:RTE:RTE:64::4                       4      18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05        2001:RTE:RTE:64::4                       4      18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06        2001:RTE:RTE:64::4                       4      18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07        2001:RTE:RTE:64::4                       4      18:24:04

Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)

cisco-NXT-FAR5#show wpan 4/1 rpl itable
```

```
        ------------------------------ WPAN RPL IPROUTE INFO TABLE [4] ------------------------------
NODE_IPADDR                    RANK  VERSION     NEXTHOP_IP                      ETX_P      ETX_LRSSIR  RSSIF HOPS  PARENTS      SSLOT
2001:RTE:RTE:64:207:8108:3C:1800        835   1     2001:RTE:RTE:64::4                        0     762   -67   -71   1     1      3
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        692   2     2001:RTE:RTE:64::4                        0     547   -68   -67   1     1      3
2001:RTE:RTE:64:207:8108:3C:1802        776   2     2001:RTE:RTE:64::4                        0     711   -82   -83   1     1      3
2001:RTE:RTE:64:207:8108:3C:1803        968   2     2001:RTE:RTE:64::4                        0     968   -72   -63   1     1      3
2001:RTE:RTE:64:207:8108:3C:1804        699   1     2001:RTE:RTE:64::4                        0     643   -71   -66   1     1      3
2001:RTE:RTE:64:207:8108:3C:1805        681   1     2001:RTE:RTE:64::4                        0     627   -70   -64   1     1      3
2001:RTE:RTE:64:207:8108:3C:1806        744   1     2001:RTE:RTE:64::4                        0     683   -69   -68   1     1      3
2001:RTE:RTE:64:207:8108:3C:1807        705   1     2001:RTE:RTE:64::4                        0     648   -76   -63   1     1      3
2001:RTE:RTE:64:207:8108:3C:1808        811   2     2001:RTE:RTE:64::4                        0     811   -68   -69   1     2      3
2001:RTE:RTE:64:207:8108:3C:1809        730   1     2001:RTE:RTE:64::4                        0     692   -68   -70   1     1      3
2001:RTE:RTE:64:207:8108:3C:180A        926   1     2001:RTE:RTE:64::4                        0     926   -66   -68   1     1      3
2001:RTE:RTE:64:207:8108:3C:180B        602   2     2001:RTE:RTE:64::4                        0     314   -74   -69   1     1      3
2001:RTE:RTE:64:207:8108:3C:1A00        948   1     2001:RTE:RTE:64:207:8108:3C:1801        692   256   -73   -75   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A01        646   2     2001:RTE:RTE:64:207:8108:3C:180B        323   256   -73   -75   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A02        948   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -73   -75   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A03        803   2     2001:RTE:RTE:64:207:8108:3C:1805        503   256   -68   -78   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A04        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -65   -69   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A05        646   2     2001:RTE:RTE:64:207:8108:3C:180B        323   256   -71   -69   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A06        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -73   -75   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A07        979   1     2001:RTE:RTE:64:207:8108:3C:1805        627   352   -71   -73   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A08        646   2     2001:RTE:RTE:64:207:8108:3C:180B        390   256   -75   -70   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A09        948   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -70   -69   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A0A        646   2     2001:RTE:RTE:64:207:8108:3C:180B        390   256   -75   -71   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A0B        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -68   -68   2     2      3
2001:RTE:RTE:64:207:8108:3C:1C00        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -70   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C01        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -71   -72   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C02        1114  1     2001:RTE:RTE:64:207:8108:3C:1A06        858   256   -74   -73   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C03        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -76   -77   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C04        902   2     2001:RTE:RTE:64:207:8108:3C:1A06        646   256   -75   -68   3     2      3
2001:RTE:RTE:64:207:8108:3C:1C05        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -66   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C06        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -74   -72   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C07        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -70   -75   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C08        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -74   -70   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C09        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -70   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C0A        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -70   -69   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C0B        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -76   -74   3     1      3
2001:RTE:RTE:64:217:3BCD:26:4E00        616   2     2001:RTE:RTE:64::4                        0     616   118   118   1     1      4     // CY PLC
nodes
2001:RTE:RTE:64:217:3BCD:26:4E01        702   1     2001:RTE:RTE:64::4                        0     646   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E02        557   2     2001:RTE:RTE:64::4                        0     557   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E03        626   1     2001:RTE:RTE:64::4                        0     579   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E04        609   2     2001:RTE:RTE:64::4                        0     609   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E05        602   2     2001:RTE:RTE:64::4                        0     602   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E06        594   2     2001:RTE:RTE:64::4                        0     594   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E07        584   2     2001:RTE:RTE:64::4                        0     584   118   118   1     1      4

        Number of Entries in WPAN RPL IPROUTE INFO TABLE: 44

        cisco-NXT-FAR5#

        cisco-NXT-FAR5#show run int wpan 4/1
        Building configuration...
        Current configuration : 320 bytes
        !
        interface Wpan4/1
         no ip address
         ip broadcast-address 0.0.0.0
         no ip route-cache
         ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
         ieee154 panid 5552
         ieee154 ssid ios_far5_plc
         ipv6 address 2001:RTE:RTE:64::4/64
         ipv6 enable
         ipv6 dhcp relay destination  2001:420:7BF:5F::500
        end

        cisco-NXT-FAR5#show run int wpan 3/1
        Building configuration...
        Current configuration : 333 bytes
        !
        interface Wpan3/1
         no ip address
         ip broadcast-address 0.0.0.0
         no ip route-cache
```

```
 ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
 ieee154 panid 5551
 ieee154 ssid ios_far5_rf
 slave-mode 4
 ipv6 address 2001:RTE:RTE:65::5/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end
```

IoT FND データベースのバックアップと復元

ここでは、IoT FND がデータベースの完全バックアップと増分バックアップをどのようにサポートしているかを説明します。

はじめる前に

IoT FND データベースをバックアップする前に、次の手順を実行します。

1. 最新の cgms-oracle-*version_number*.x86_64.rpm パッケージをダウンロードしてインストールします。
2. スクリプト、テンプレート、ツール フォルダを /opt/cgms-oracle フォルダから $ORACLE_BASE/cgms フォルダにコピーします。
3. oracle:dba にコピーしたファイルとフォルダの所有権を設定します。

IoT FND データベースの完全バックアップの作成

完全バックアップは、データ ファイルからすべてのブロックをバックアップします。完全バックアップは時間がかかり、部分バックアップより多くのディスク領域とシステム リソースを消費します。

IoT FND では、IoT FND データベースの完全なホット バックアップを実行できます。ホット バックアップでは、IoT FND および IoT FND データベースはバックアップ中も動作します。

(注) バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

IoT FND ソフトウェアのバックアップ ファイルを作成するには、次の手順を実行します。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ oracle に切り替えます。

   su - oracle

3. ディレクトリを IoT FND バックアップ スクリプト（backupCgmsDb.sh）の場所に変更します。

   cd /home/oracle/app/oracle/cgms/scripts

4. バックアップ スクリプトを実行し、バックアップ先フォルダを指定します。たとえば、/home/oracle/bkp フォルダにバックアップ データを保存するには、次のコマンドを入力します。

   ```
   ./backupCgmsDb.sh full /home/oracle/bkp
   08-03-2012 15:54:10 PST: INFO: ========== CGMS Database Backup Started ==========
   08-03-2012 15:54:10 PST: INFO: Log file: /tmp/cgms_backup_restore.log
   Are you sure you want to backup CG-NMS database (y/n)? y
   ```

5. バックアップ プロセスを開始するには、「y」を入力します。

IoT FND の完全バックアップのスケジュール設定

IoT FND の完全バックアップを毎日 1:00 AM（デフォルト設定）に実行するようにスケジュール設定するには、次の手順を実行します。

（注）バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ *oracle* に切り替えます。

   ```
   su - oracle
   ```

3. ディレクトリを IoT FND バックアップ スクリプト（backupCgmsDb.sh）の場所に変更します。

   ```
   cd /home/oracle/app/oracle/cgms/scripts
   ```

4. バックアップ スクリプトを実行し、バックアップ先フォルダを指定します。

バックアップのスケジュール間隔を変更するには、installCgmsBackupJob.sh スクリプトを編集してから実行します。たとえば、バックアップ データを /home/oracle/bkp に保存するには、次のコマンドを入力します。

```
./installCgmsBackupJob.sh /home/oracle/bkp
```

バックアップ ジョブを削除するには、次のコマンドを入力します。

```
cd /home/oracle/app/oracle/cgms/scripts
./deinstallCgmsBackupJob.sh
```

IoT FND データベースの増分バックアップ

増分バックアップは、前回指定したバックアップから変更されたデータ ファイル ブロックのみをバックアップします。IoT FND は 2 つのレベルの増分バックアップと、毎時のログ バックアップをサポートしています。

- incr0：増分バックアップ後のベース バックアップ。これは完全バックアップに似ています。大規模展開（数百万のメッシュ エンドポイントと数千の FAR）の場合、週に 2 回 incr0 バックアップを実行します。
- incr1：前回の増分バックアップ以降に変更されたすべてのブロックの差分バックアップ。大規模展開（数百万のメッシュ エンドポイントと数千の FAR）の場合、1 日に 1 回 incr1 バックアップを実行します。

（注）incr1 差分バックアップのベースを確立するため、incr0 バックアップを incr1 バックアップの前に実行する必要があります。

- 毎時のアーカイブ ログのバックアップ：Oracle データベースは、アーカイブ ログを使用してデータベースへのすべての変更を記録します。これらのファイルは徐々に増え、大量のディスク領域を消費する可能性があります。1 時間ごとに backup_archive_log.sh スクリプトを実行するようにスケジュール設定します。このスクリプトはデータベースのアーカイブ（.arc）ログ ファイルをバックアップし、それらを別のサーバに保存し、元のアーカイブ ログ ファイルを削除してデータベース サーバの領域を解放します。

  ヒント：IoT FND データベースに多くの変更を及ぼす重大な操作（百万のメッシュ エンドポイントをインポートしたり、メッシュ エンドポイントにファームウェア イメージをアップロードするなど）を実行する前に、incr0 バックアップを実行します。操作が完了したら、別の incr0 バックアップを実行してから、スケジュール設定された増分バックアップを再開します。

増分バックアップの実行

(注)バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

増分バックアップを実行するには、次の手順を実行します。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ *oracle* に切り替え、IoT FND バックアップ スクリプトの場所にディレクトリを変更します。

```
su - oracle
cd /home/oracle/app/oracle/cgms/scripts
```

3. バックアップ スクリプトを実行し、増分バックアップのレベルとバックアップ データを保存する保存先フォルダ(/home/oracle/bkp など)を指定します。たとえば、/home/oracle/bkp への incr0 バックアップを実行するには、次のコマンドを入力します。

```
./backupCgmsDb.sh incr0 /home/oracle/bkp
```

incr1 バックアップを実行するには、次のコマンドを入力します。

```
./backupCgmsDb.sh incr1 /home/oracle/bkp
```

IoT FND バックアップの復元

cgms-oracle.rpm パッケージで提供されるスクリプトを使用して、データベースのバックアップと復元を実行します。提供されたスクリプトを使用している場合、バックアップと復元は Oracle データベースの同じバージョンで実行された場合にのみ機能します。

(注)提供されたスクリプトを使用している場合、Oracle バージョン 11.2.0.1 からのバックアップは、v11.2.0.1 でのみ復元できます。Oracle の異なるバージョン間でのバックアップは機能しません。たとえば、11.2.0.1 で作成されたバックアップは、提供されたスクリプトを使用して 11.2.0.3 で復元することはできません。データベースを 11.2.0.1 から 11.2.0.3 にアップグレードする必要がある場合は、Oracle のアップグレード手順に従います。Oracle のアップグレード マニュアルおよび Web サイトを参照してください。

IoT FND は同じホストまたは別のホストでの IoT FND バックアップの復元をサポートしています。IoT FND バックアップを別のホストに復元する場合は、そのホストで Oracle データベース ソフトウェアの同じかそれ以降のバージョンが実行され、復元先のホストで IoT FND データベースが setupCgmsDb.sh スクリプトを使用して作成されていることを確認します。

(注)IoT FND ではクロスプラットフォーム バックアップはサポートしていません。

IoT FND バックアップを復元するには、次の手順を実行します。

1. IoT FND を停止します。

```
service cgms stop
```

2. ユーザ oracle に切り替え、スクリプトの場所にディレクトリを変更し、Oracle を停止します。

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./stopOracle.sh
```

3. IoT FND データベースを復元するには、次のコマンドを実行します。

```
./restoreCgmsDb.sh full-backup-file
```

ヒント:完全バックアップからの復元の実行には時間がかかる場合があります。大規模展開では、増分バックアップからのデータベースを復元することを推奨します。

増分バックアップから IoT FND データベースを復元するには、次のコマンドを実行して、前回の増分バックアップ ファイルへのパスを指定します。

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./restoreCgmsDb.sh last-incr1-backup-file
```

復元スクリプトで次のエラーが表示される場合があります。

```
06-08-2012 13:12:56 PDT: INFO: Import completed successfully
06-08-2012 13:12:56 PDT: INFO: Shared memory file system.Required (1K-blocks): 6084456,
Available (1K-blocks): 4083180
06-08-2012 13:12:56 PDT: ERROR: Insufficient shared memory file system.Increase your
shared memory file system before restoring this database.
06-08-2012 13:12:56 PDT: ERROR: ========== CGMS Database Restore Failed ==========
06-08-2012 13:12:56 PDT: ERROR: Check log file for more information.
```

これらのエラーを避けるには、共有メモリ ファイル システムのサイズを増やします。

```
###### as "root" user
###### Following command allocates 6G to shm.Adjust size as needed.
# umount tmpfs
# mount -t tmpfs tmpfs -o size=6G /dev/shm

###### Edit /etc/fstab and replace defaults as shown below
tmpfs                   /dev/shm                tmpfs   size=6G        0 0
```

4. Oracle を起動します。

```
./startOracle.sh
```

5. ディレクトリを /opt/cgms に変更し、db-migrate スクリプトを実行します。

```
$ cd /opt/cgms
$ bin/db-migrate
```

IoT FND データベースを復元すると、復元スクリプトによってデータベースはデータベースが使用していた IoT FND のバージョンに復元されます。古いデータベースを IoT FND の新しいバージョンに復元するとエラーが返されます。移行スクリプトを実行して、データベースが IoT FND の現在のバージョンで実行されていることを確認します。

6. IoT FND を起動します。

```
service cgms start
```

ディザスタ リカバリについては、クリーンな復元を実行します。スクリプトは最初に現在の IoT FND データベースを削除します。

```
$ su -oracle
$ cd /home/oracle/app/oracle/cgms/scripts
$ ./deleteCgmsDb.sh
INFO: ======== CGMS Database Deletion Started - 2011-10-16-07-24-09 ==========
INFO: Log file: /tmp/cgmsdb_setup.log
INFO: Deleting database.This may take a while.Please be patient ...
INFO: Delete database completed successfully
INFO: ========== CGMS Database Deletion Completed Successfully - 2011-10-16-07-25-01 ==========
```

クリーンな復元が必要ない場合は、Oracle ツールを使用してデータベースを復元します。

ESX 5.x での IoT FND/Oracle/TPS 仮想マシンの展開

VMware vSphere Client を使用して、OVA ファイルを ESXi 5.x. にインポートします。

はじめる前に

- ESXi 5.x サーバ用の VMware vSphere Client をインストールします。

- VMware ESXi 5.x のクレデンシャルを見つけて ESXi 5.x で仮想マシンを作成します。
- VMware サーバ マシンの要件を満たしていることを確認します。

  以下は小規模展開の VM CPU とメモリの要件です。

  NMS OVA

  - 16 GB のメモリ
  - 1 つのコアと 4 つの仮想ソケット
  - 150 GB の仮想ストレージ

  Oracle OVA

  - 24 GB のメモリ
  - 2 つの仮想ソケットとソケットあたり 2 つのコア
  - 300 GB の仮想ストレージ

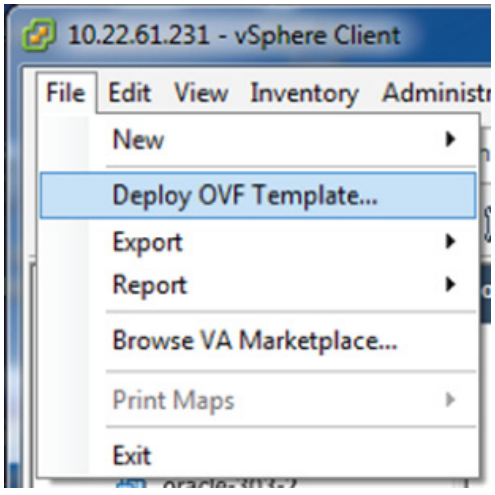
  TPS OVA

  - 4 GB のメモリ
  - 1 つの仮想ソケットと 1 つのコア
  - 50 GB の仮想ストレージ

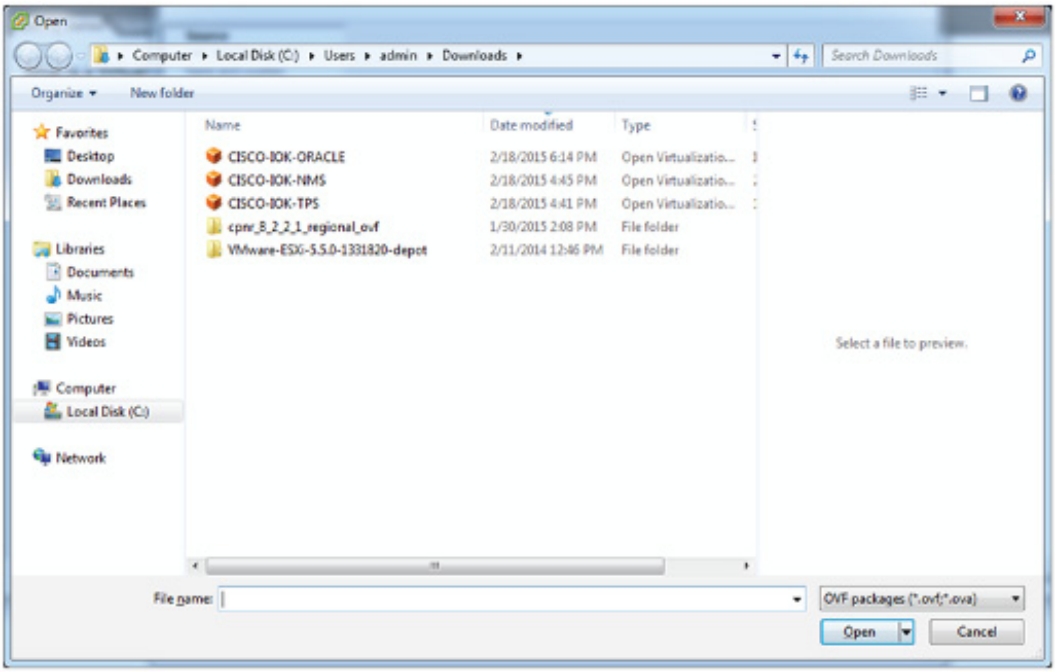
手順の詳細

VMware vSphere Client 5.x を使用して、IoT FND、Oracle、および TPS 仮想アプライアンスを ESXi 5.x にインポートするには、次の手順を実行します。

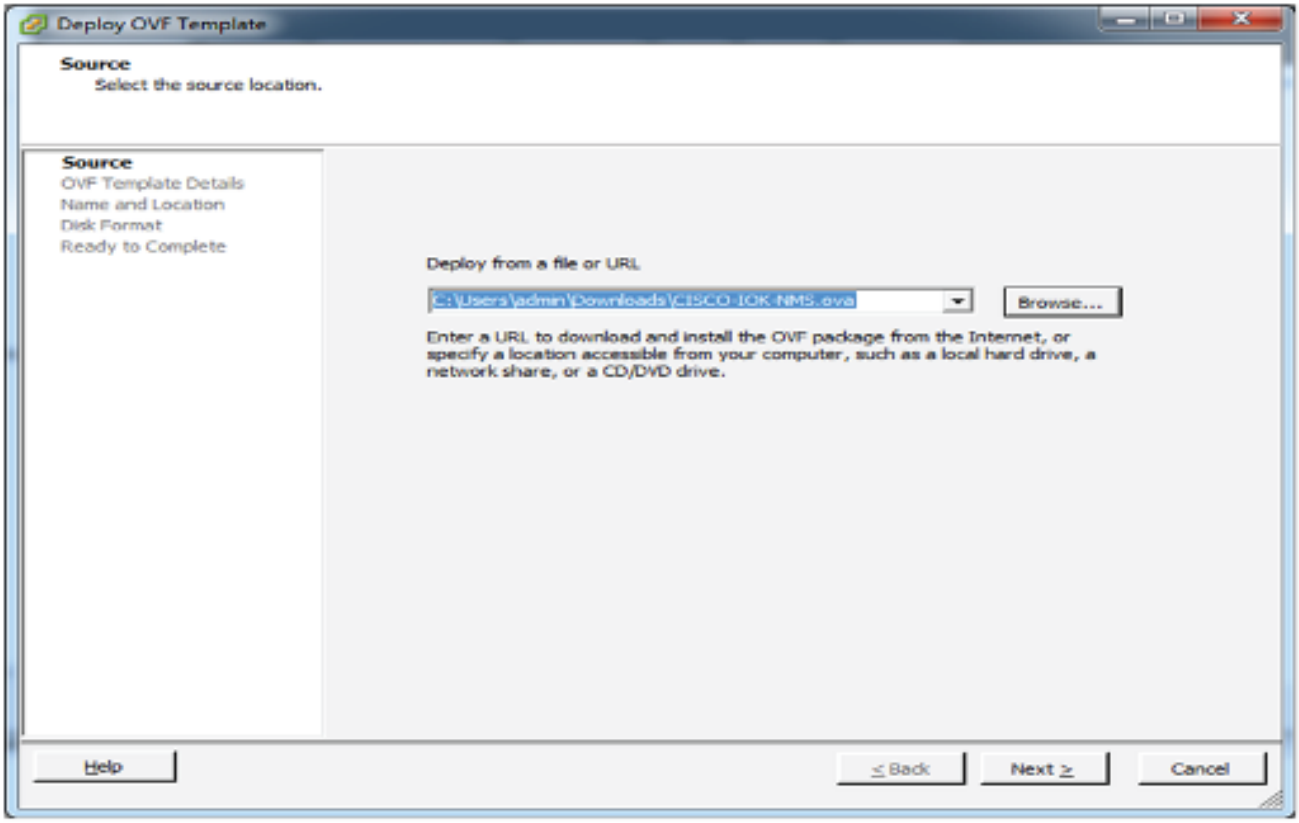
1. VMware vSphere Client にログインします。
2. [File] > [Deploy OVF Template...] の順に選択します。



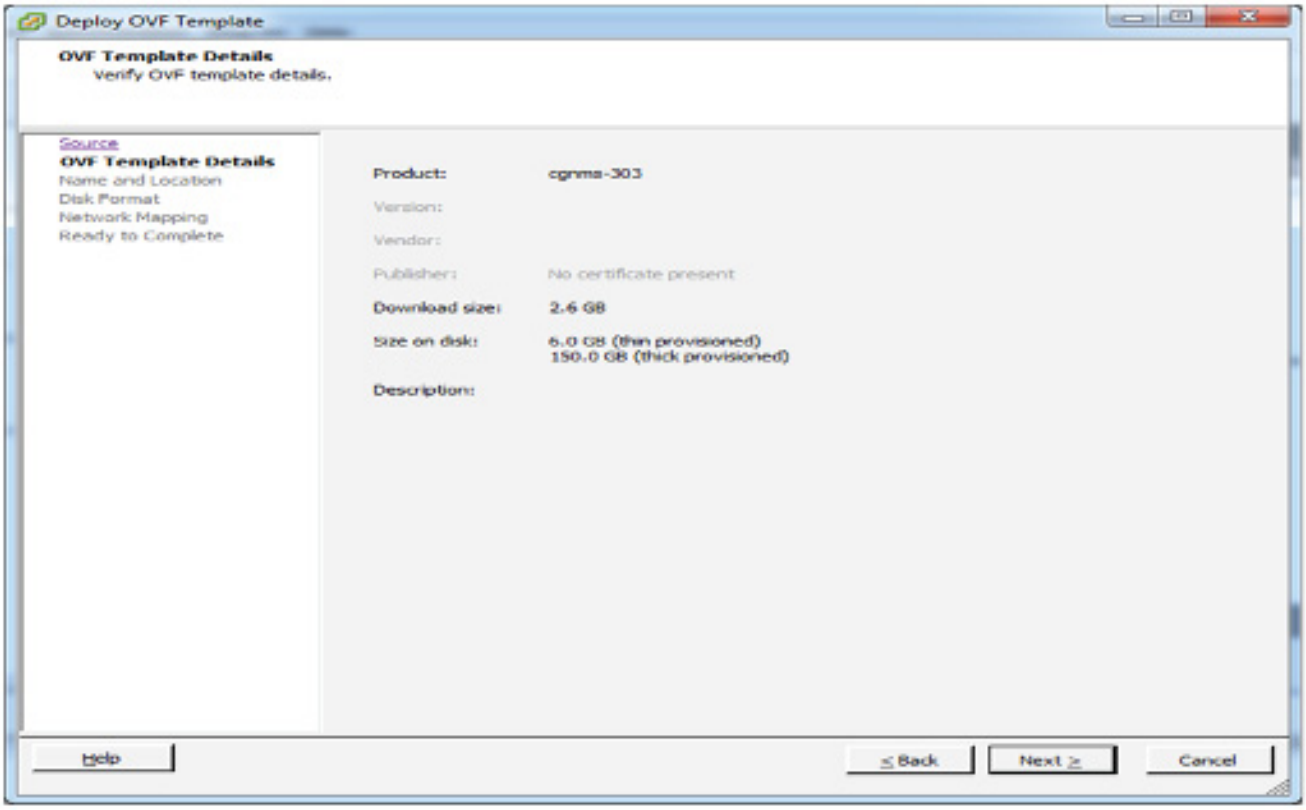
3. CISCO-IOK-NMS.ova ファイルを参照し、[Open] をクリックします。



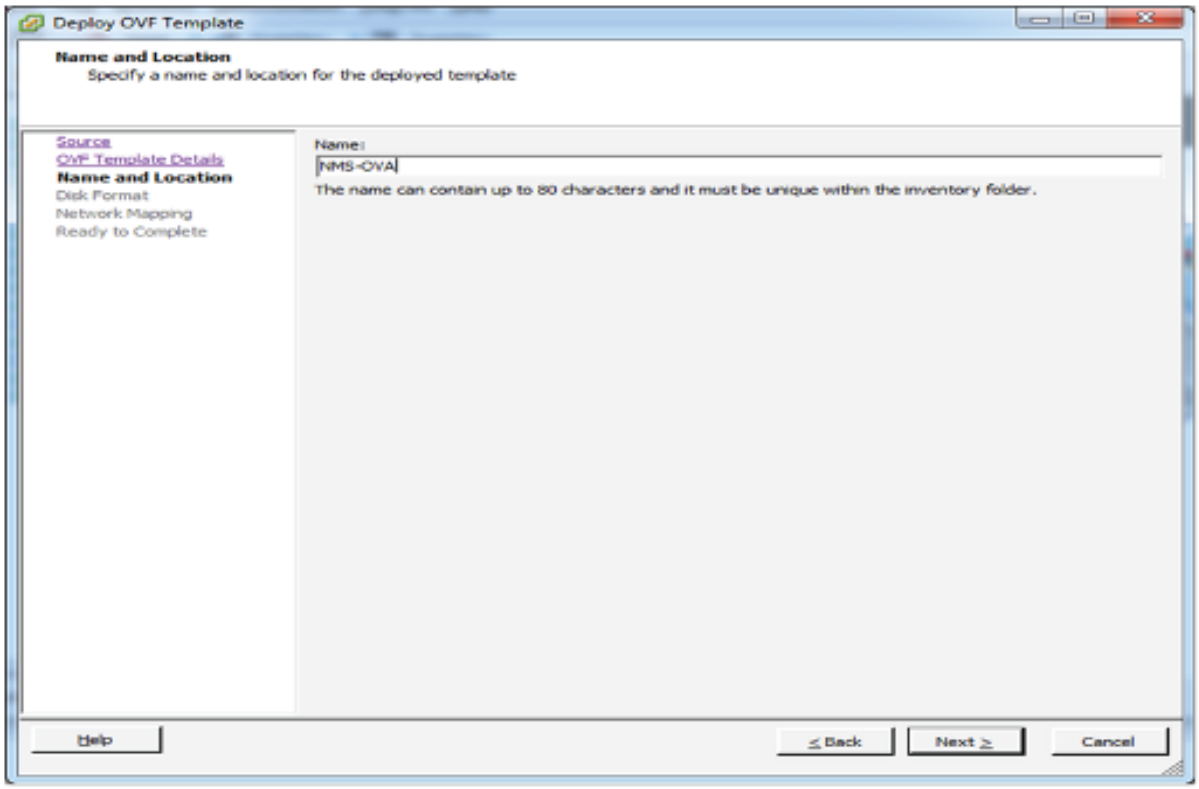
4. [Source] ウィンドウに正しい OVA ファイルが表示されていることを確認し、[Next] をクリックします。



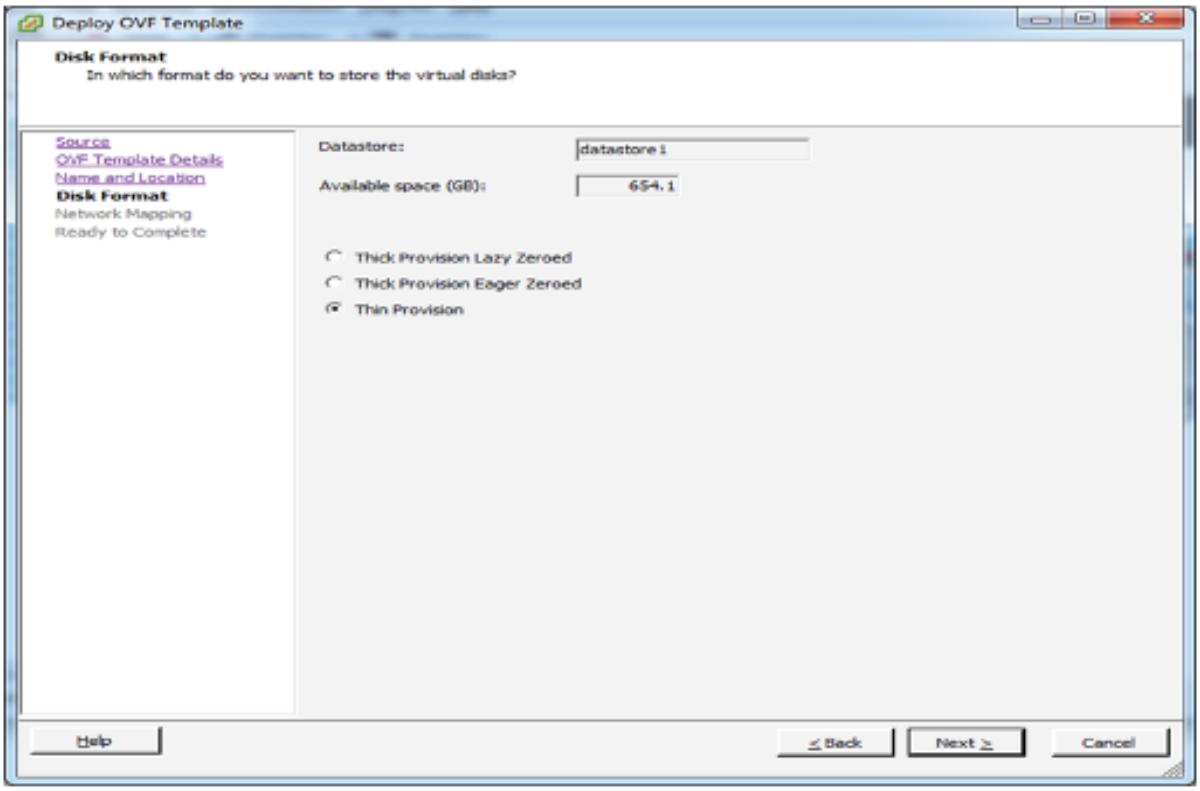
5. [OVF Template Details] ウィンドウで、情報を確認して [Next] をクリックします。



6. [Name and Location] ウィンドウで、この仮想アプライアンスの名前を入力し、[Next] をクリックします。

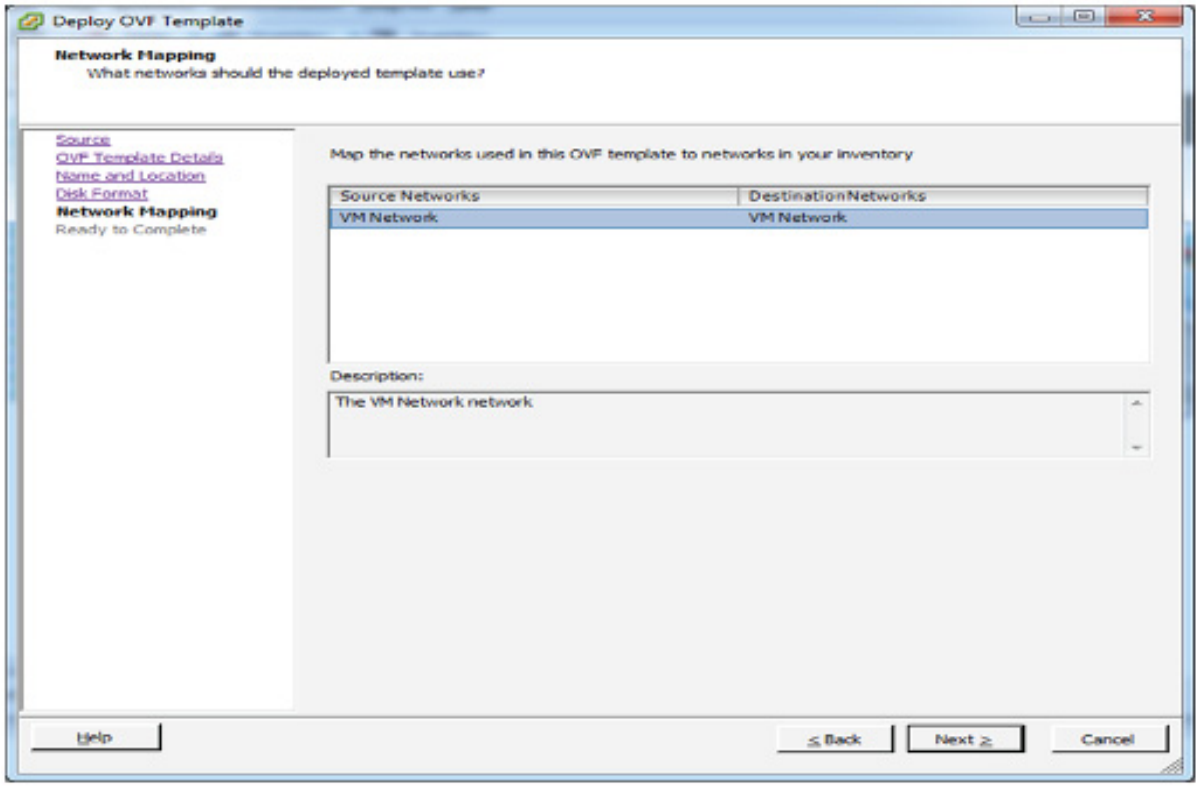


7. [Disk Format] ウィンドウで、[Thin Provision] を選択し、[Next] をクリックします。

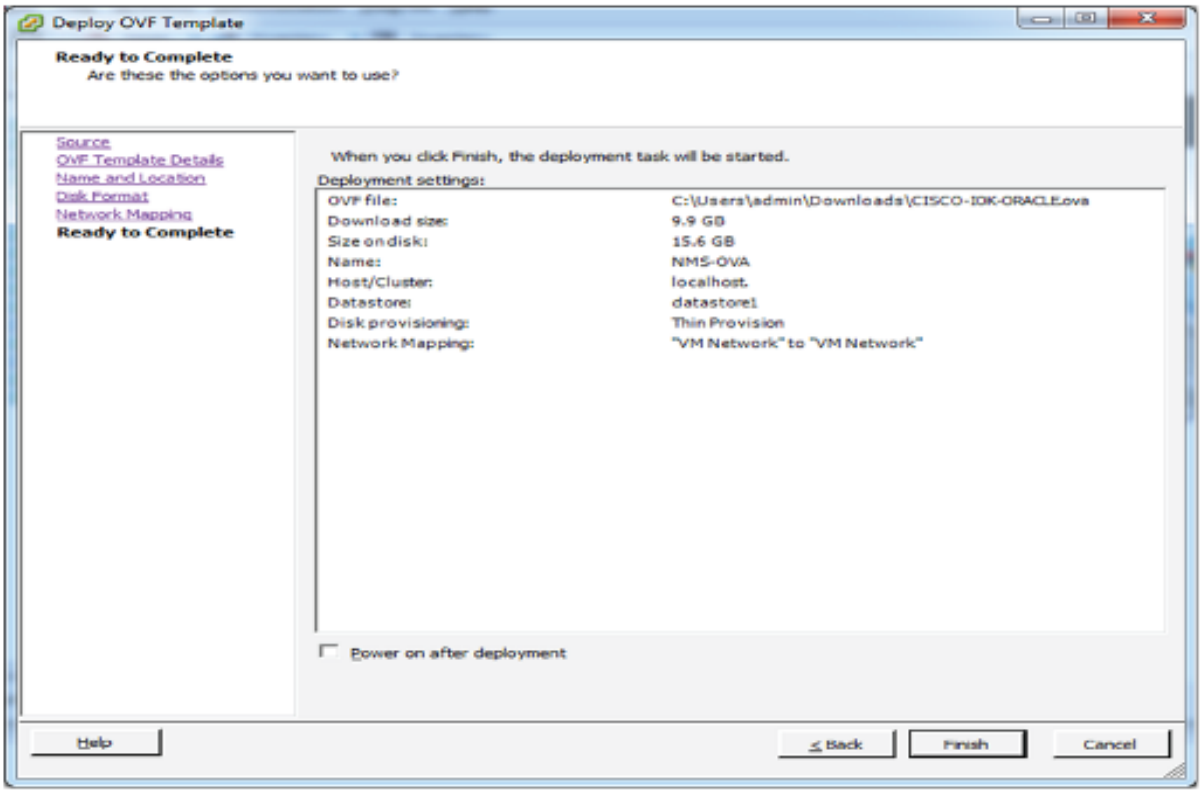


シン プロビジョニングでは、VM ディスクを必要に応じて大きくすることができます。

8. [Network Mapping] ウィンドウで、[Source Network] を選択し、[Next] をクリックします。



9. [Ready to Complete] ウィンドウで、展開設定を確認し、[Finish] をクリックします。

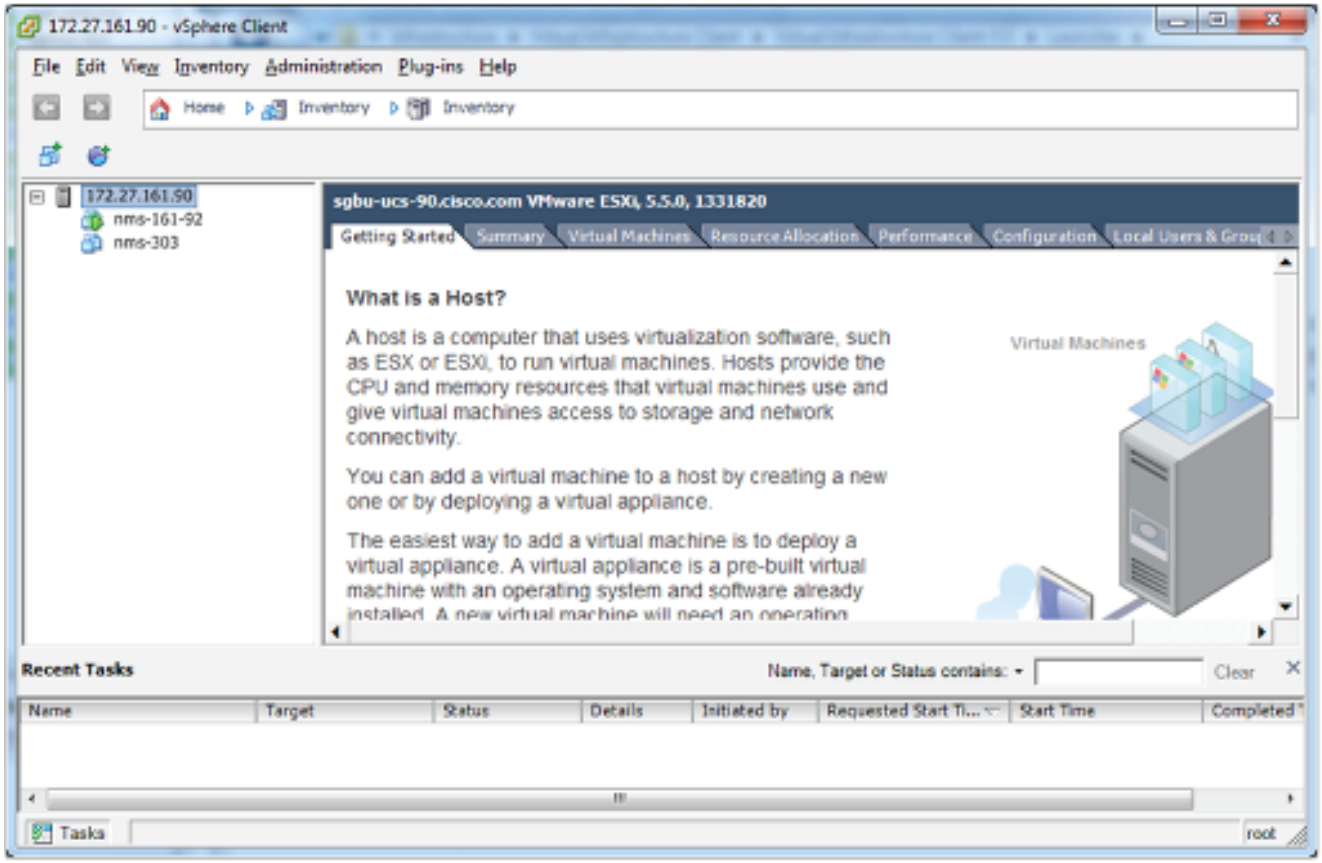


VM は現在、データストアにあります。

10. vSphere Client にログインしている間、上記の手順を繰り返して CISCO-IOK-ORACLE ファイルと CISCO-IOK-TPS OVA ファイルを展開します。

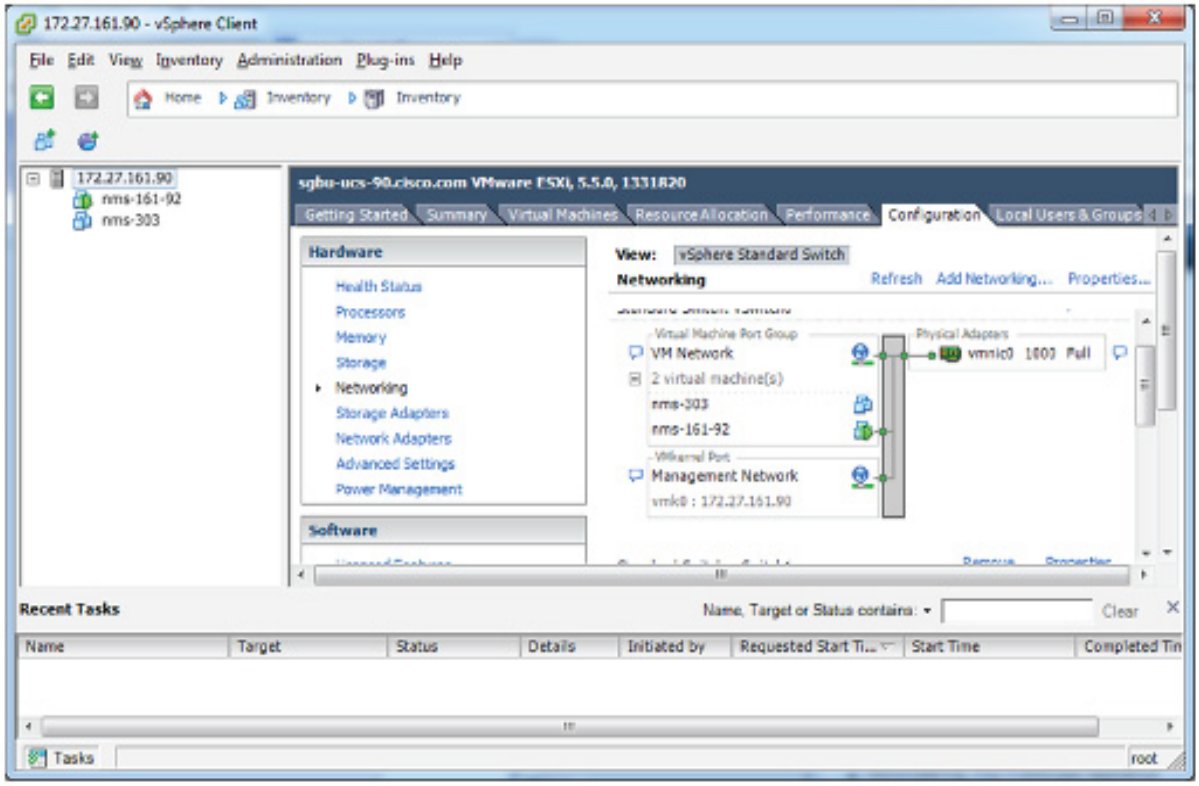
11. すべての新しい OVA アプライアンスを VM ネットワークに追加します。

    次の vSphere Client のホーム画面には、nms アプライアンスが示されています。

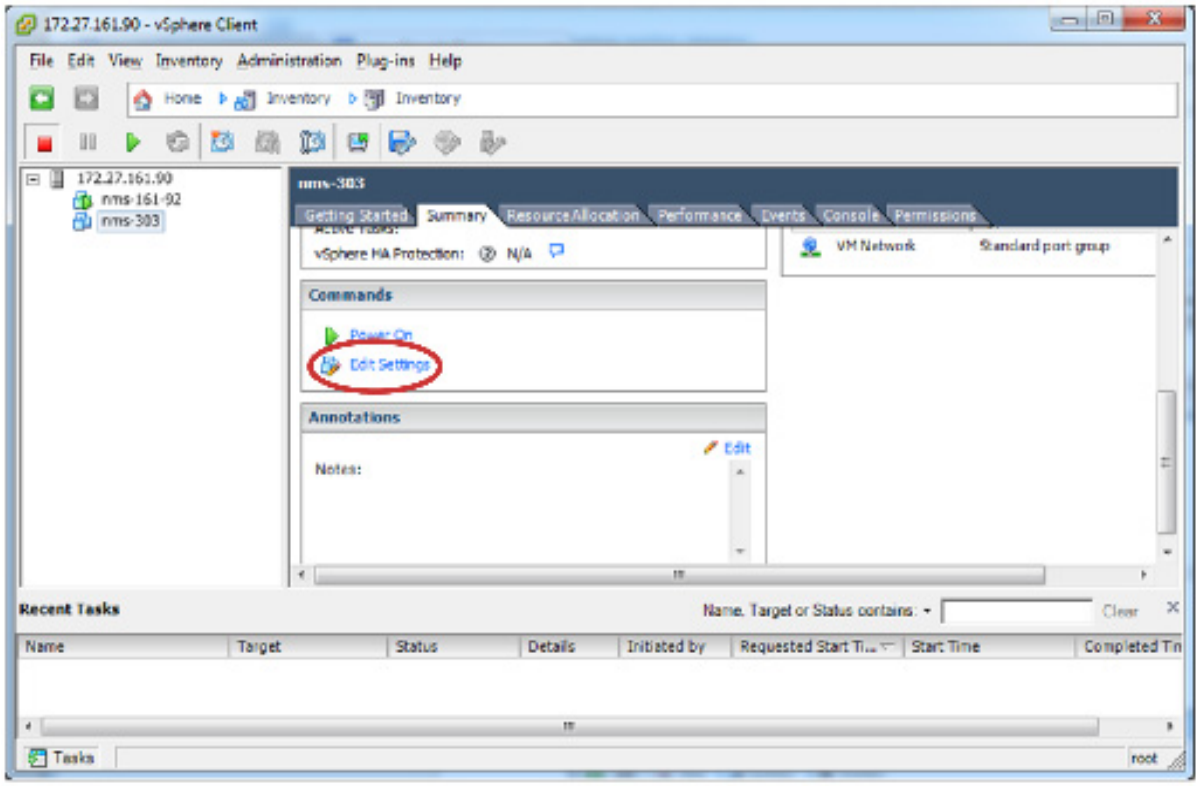


12. [Configuration] タブを選択して、この選択した ESXi サーバのネットワーク プロパティを表示します。

    ネットワーク プロパティは、サーバの要件によって異なります。以下は、管理ネットワーク接続用の vSphere Standard Network Switch と VM Network ラベルを示しています。

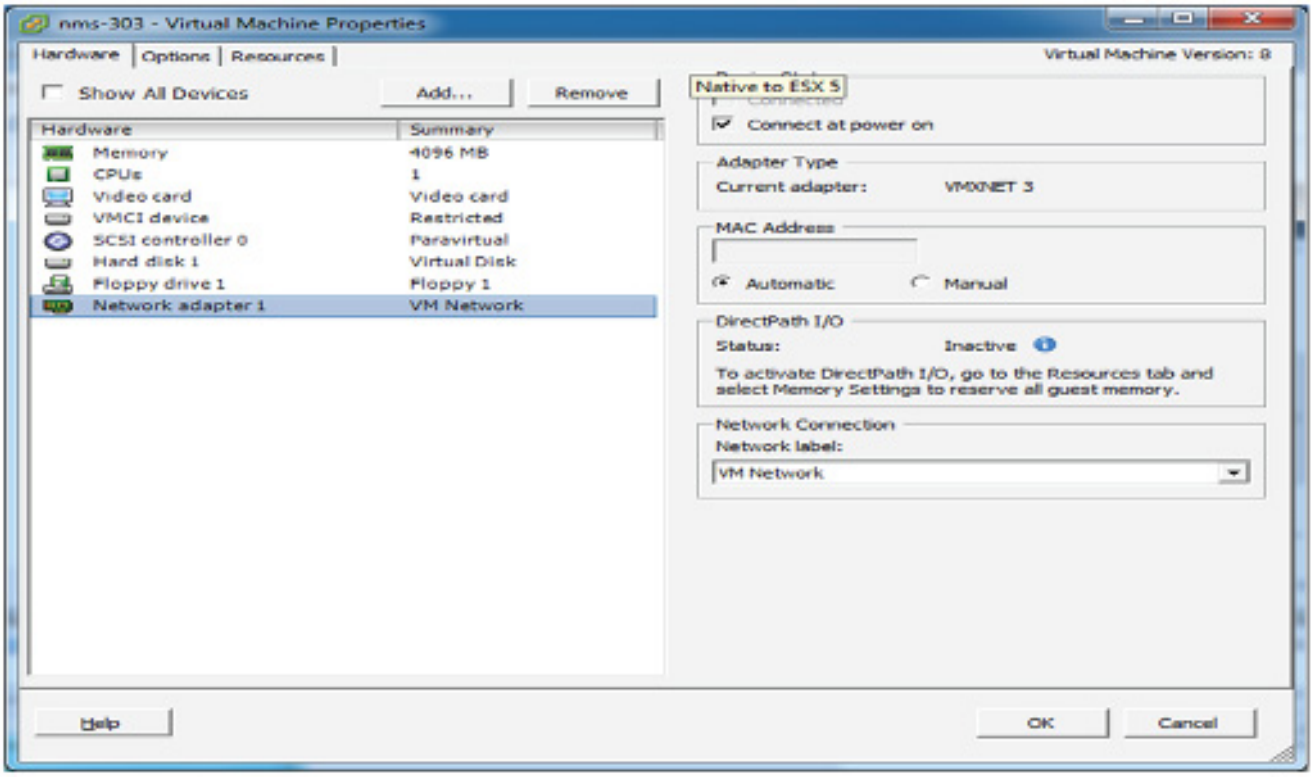


13. 左側のパネルで、[nms 303] アプライアンスを選択し、[Summary] タブを選択します。
14. [Command] セクションまでスクロールし、[Edit Settings] をクリックします。



[Virtual Machine Properties] ページが表示されます。

15. [Hardware] タブの [Network Connection] セクションで、ネットワーク アダプタを選択し、[Network label] ドロップダウン メニューから [VM Network] ラベル（または作成したネットワーク ラベル）を選択します。



16. [OK] をクリックします。

    ネットワーク ラベルはユーザ設定に保存されます。

17. nms インスタンスを右クリックして、コンテキスト メニューから [Open Console] を選択します。

18. 緑色の [Play] ボタンをクリックします。

    Linux VM を開始して起動します。

    Linux のブート メッセージが表示され、ログイン画面が表示されます。

    VM コンソールを終了するには、Ctrl キーを押した状態で Alt キーを押します。

19. 画面の中央をクリックしてログインし、IP アドレスの設定を調整します。

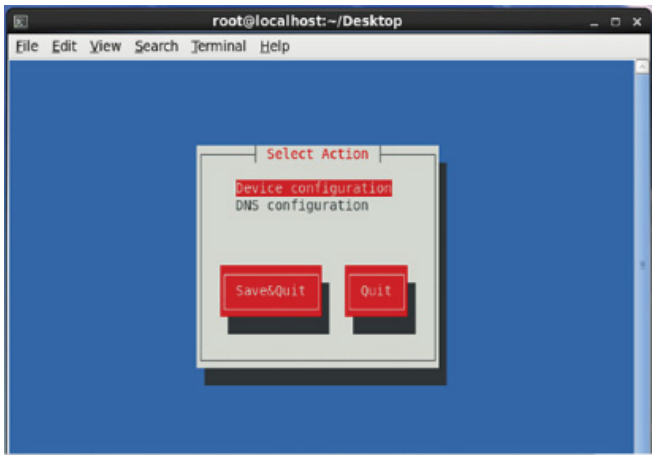
    これは他の RedHat 6.4 Enterprise System と同じです。

20. Oracle と TPS アプライアンスに対して、ステップ 12 ～ 19 を繰り返します。

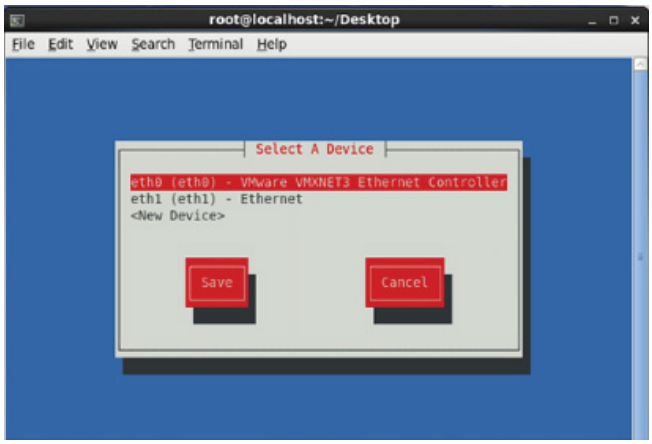
VM 内でのネットワーク構成ファイルの編集

1. デスクトップを右クリックし、[Open in Terminal] をクリックします。
2. コマンド プロンプトで、「**system-config-network**」を入力します。

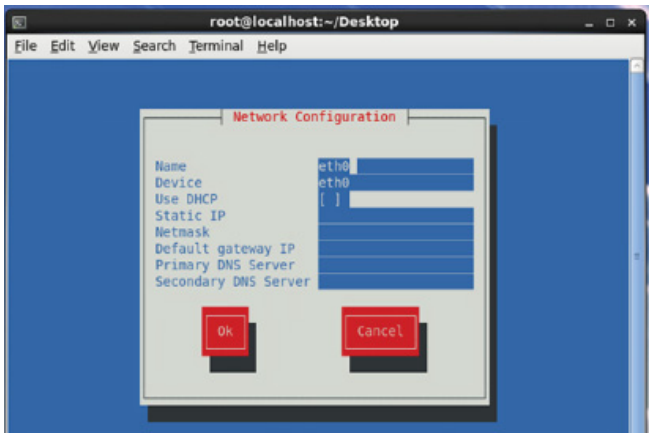
   [Device configuration] ウィンドウが表示されます。



3. [Select Action] ウィンドウで、[Device configuration] が選択されていることを確認し、**Enter** キーを押します。
4. [Select A Device] ウィンドウで、方向キーを使用してインターフェイスを選択し、Enter キーを押します。



次の例では、[Network Configuration] ウィンドウで [DHCP] が選択されています。



5. ネットワーク管理者によって割り当てられたネットワーク設定を入力します。
6. [OK] をクリックします。
7. アプライアンスごとにステップ 1 ～ 5 を繰り返して IP アドレスを割り当てます。

証明書の生成およびインストール

この項では、デジタル証明書を生成してインストールする方法について説明します。次の項目を取り上げます。

証明書について

ここでは、証明書について説明します。

証明書の役割

Cisco 1000 シリーズ Connected Grid ルータ（CGR 1000 または単に CGR）と Cisco Connected IoT Field Network Director（IoT FND）との間のすべての通信は、両方向とも相互認証により認証される必要があります。相互認証が行われる前に、Cisco IoT FND および CGR は、それぞれ同じ認証局（CA）により署名される必要があります。ルート CA またはや下位 CA（subCA）のいずれかを採用できます。

CGR の証明書の生成について詳しくは、『Certificate Enrollment Guide for the Cisco 1000 Series Connected Grid Routers』を参照してください。

IoT FND の証明書の生成には、IoT FND TPS プロキシ（tpsproxy）の証明書の生成と読み込みも関係しています。証明書を生成したら、それらを TPS プロキシと キーストア として知られている IoT FND 上のストレージ場所にインポートします。

キーストア

Keystore により、特定のシステム（IoT FND や TPS プロキシなど）の詳細が提供され、それには次の項目が含まれています。

- そのシステムの証明書（IoT FND 証明書または TPS プロキシ証明書など）
- システムの秘密キー
- 証明書チェーン（CA または subCA へのパス）

IoT FND キーおよび証明書は、IoT FND サーバ上の /opt/cgms/server/cgms/conf/ ディレクトリ内の cgms_keystore ファイルに 格納されます。

証明書の生成およびエクスポート

(注) IoT FND 証明書は、データベースのデータを暗号化します。**この証明書は決して消失させないでください。**この証明書を消失すると、一部のデータベース データが復号できなくなります。

証明書を生成してエクスポートするには、次の手順を実行します。

- IoT FND および TPS プロキシの証明書テンプレートの設定IoT FND
- 証明書テンプレートの有効化
- IoT FND および IoT FND TPS プロキシの証明書の生成
- コマンド認可サポート
- HSM のカスタム CA の設定
- SSM のカスタム CA の設定
- CA 証明書のエクスポート

IoT FND および TPS プロキシの証明書テンプレートの設定IoT FND

CA（または subCA）上で、IoT FND と TPS プロキシの証明書を生成する証明書テンプレートを作成する必要があります。

証明書テンプレートを作成するには、次の手順を実行します。

1. Windows Server 2008 R2 Enterprise エディションを稼働するシステム上で、認証局アプリケーションを開きます。

認証局アプリケーションは、上記の Windows Server バージョン上では標準です。

2. メニューを展開して、証明書テンプレート フォルダを表示します。
3. [Certificate Templates] を右クリックし、コンテキスト メニューから [Manage] を選択します。
4. 右ペインで [Computer] を右クリックし、コンテキスト メニューから [Duplicate Template] を選択し、[NMS] を入力します。
5. [Duplicate Template] ペインで、[Windows Server 2008 Enterprise] を選択します。
6. [OK] をクリックします。
7. [NMS Properties] > [General] タブをクリックし、次の手順を実行します。
   a. [Template display name] と [Template name] フィールドに、**NMS** を入力します。
   b. 適切な [Validity] を入力します。これは証明書の存続期間を定義します。
   c. [Publish certificate in Active Directory] チェックボックスをオンにします。
   d. [OK] をクリックします。
8. [NMS Properties] > [Extensions] タブをクリックし、次の手順を実行します。
   a. [Extensions] ペインで、[Application Policies] を選択します。
   b. [Application Policies] ペインで、クライアント認証とサーバ認証が下部のペインに表示されていることを確認します。
   c. 上部の [Extensions] ペインで [Key Usage] を選択し、[Edit] をクリックします。
   d. [Edit Key Usage Extension] ペインで、[Make this extension critical] チェックボックスをクリアします。
   e. [OK] をクリックします。

9. [NMS Properties] > [Request Handling] タブをクリックし、次の手順を実行します。
   a. [Purpose] ドロップダウン メニューから [Signature and encryption] を選択します。
   b. [Allow private key to be exported] チェックボックスをオンにします。
   c. [OK] をクリックします。
10. [NMS Properties] > [Security] タブをクリックし、次の手順を実行します。
   a. [Group] または [User Names] ペインで [Administrator] を選択します。
   b. リストされている各グループまたはユーザ名項目（認証されたユーザ、管理者、ドメイン管理者、エンタープライズ管理者など）に対して、すべての権限（フル コントロール、読み取り、書き込み、登録、自動登録）の、[Allow] チェックボックスをオンにします。
   c. [OK] をクリックします。
11. [NMS Properties] > [Cryptography] タブで、次のデフォルト設定を保持します。

- Algorithm name：RSA
- Minimum key site：2048
- Cryptographic provider：要求には、対象コンピュータ上の任意のプロバイダを使用できます
- Request hash：SHA256

12. [OK] をクリックします。
13. [NMS Properties] > [Subject Name] タブで、次のデフォルト設定を保持します。

- [Supply in the request radio button] のラジオボタンをオン
- [Use subject information from existing certificates for autoenrollment renewal requests] のチェックボックスをオン

14. [OK] をクリックします。

(注) 残りのタブ（[Superseded Templates]、[Server]、および [Issuance Requirements]）は、デフォルトの設定のままにしておきます。

証明書テンプレートの有効化

証明書を作成するには、まず証明書テンプレートを有効にする必要があります。

証明書テンプレートを有効にするには、次の手順を実行します。

1. 証明書テンプレートを設定します（証明書の生成およびエクスポートを参照）。
2. Windows Server 上で認証局アプリケーションを開きます。
3. メニューを展開して、証明書テンプレート フォルダを表示します。
4. [Certificate Templates] を右クリックし、[New] > [Certificate Template to Issue] をコンテキスト メニューから選択します。
5. [Enable Certificate Templates] ウィンドウで、[NMS] テンプレートを強調表示します。
6. [OK] をクリックします。

IoT FND および IoT FND TPS プロキシの証明書の生成

前に作成した設定テンプレートを使用して、IoT FND と TPS プロキシの証明書を生成するための同じ手順を実行します。

この項の手順を 2 回実行します。1 回は IoT FND の証明書を生成するため、もう 1 回は TPS プロキシの証明書を生成するためです。

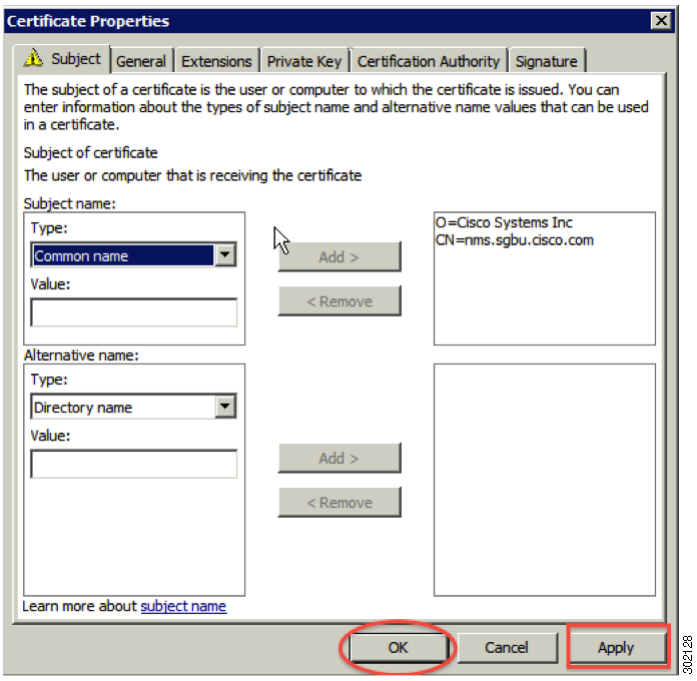
ヒント：9.b で、入力する値は、IoT FND または TPS プロキシの証明書を作成するかどうかによって異なります。

これら 2 つの証明書を作成したら、IoT FND 証明書を IoT FND アプリケーション サーバに安全に転送したり、TPS プロキシ証明書を TPS プロキシ サーバに安全にコピーしたりできます。

証明書を生成するには、次の手順に従います。

1. 証明書テンプレートを設定します（証明書の生成およびエクスポートを参照）。
2. 証明書テンプレートを有効にします（証明書テンプレートの有効化を参照）。
3. Windows Server 2008 を実行するサーバから、[Start] > [Run] を選択し、**mmc** を入力して MMC コンソールを開きます。
4. [Console 1] ウィンドウで、[Certificates] > [Personal] フォルダを展開します。
5. [Certificates] を右クリックして、コンテキスト メニューから [All Tasks] > [Request New Certificate] を選択します。
6. [Before You Begin] ウィンドウで、[Next] をクリックします。
7. [Select Certificate Enrollment Policy] ウィンドウで、[Active Directory Enrollment Policy] を選択します。[Next] をクリックします。
8. [Request Certificates] ウィンドウで、次の手順を実行します。
   a. [NMS] チェックボックスをオンにします。
   b. [More information...] リンクをクリックします。
9. [Certificate Properties] ウィンドウで、[Subject] タブをクリックし、次の手順を実行します。
   a. [Type] ドロップダウン メニューから、**[Common name (CN)]** を選択します。
   b. [Value] フィールドに、次のようにして完全修飾ドメイン名（FQDN）を追加します。
      - IoT FND 証明書の場合、導入システムの IoT FND サーバの FQDN を入力します（例：CN=nms.sgbu.cisco.com）。
      - TPS プロキシ証明書の場合、導入システムの TPS プロキシの FQDN を入力します（例：CN= tps.sgbu.cisco.com）。
   c. [Add] をクリックすると、右ペインに共通名が表示されます。
   d. [Type] ドロップダウン メニューから、**[Organization (O)]** を選択します。
   e. [Value] フィールドに、IoT FND または TPS プロキシの会社名または設定を追加します。
   f. [Add] をクリックすると、組織が右ペインに表示されます。

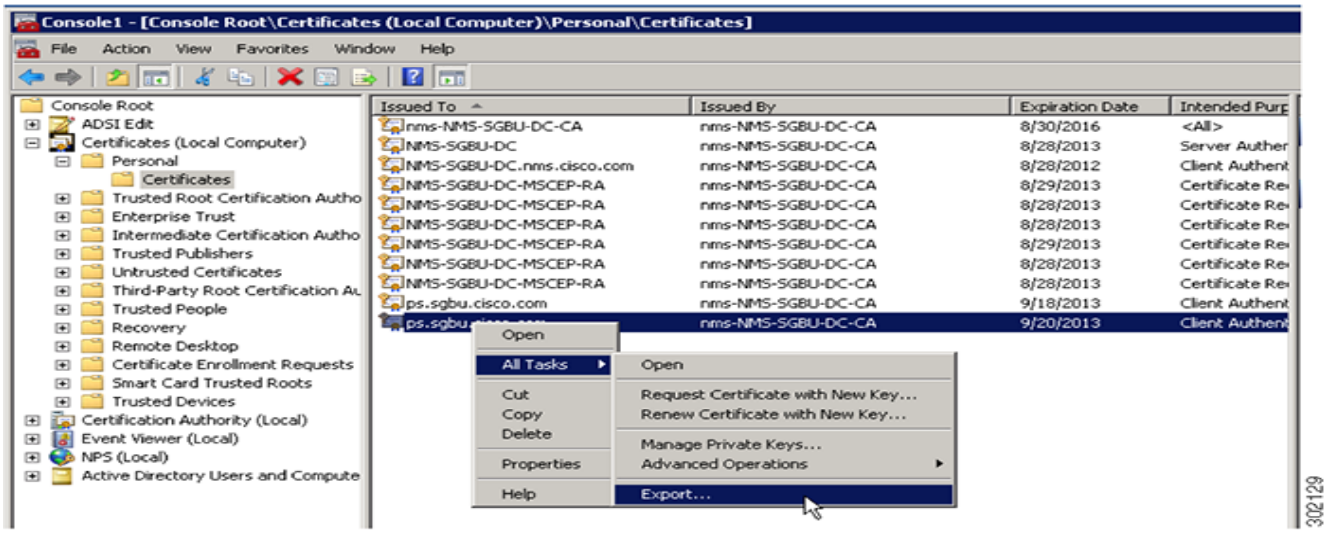
図 1　　IoT FND の共通名および組織の定義



10. [Apply] をクリックします。[OK] をクリックします。
11. [Certificate Enrollment] ウィンドウで、[NMS] チェックボックスをオンにし、[Enroll] をクリックします。
12. 登録が完了したら、[Finish] をクリックします。
13. MMC コンソール（コンソール 1）で、[Certificates] を展開します。
14. [Personal] > [Certificates] を選択します。
15. [Issued To] ペインで、新しい証明書を右クリックして、コンテキスト メニューから [All Tasks] > [Export] を選択します。

    [Export Wizard] ウィンドウが表示されます。

図 2　　サポートされる証明書を表示する [Issued To] ペイン



16. [Export Wizard] を開始します。
17. [Export Private Key] ウィンドウで、[Yes, export the private key] ラジオ ボタンを選択します。[Next] をクリックします。
18. [Export File Format] ウィンドウで、次の手順を実行します。
    a. [Personal Information Exchange] ラジオ ボタンをクリックします。
    b. [Include all certificates in the certification path if possible] チェックボックスをオンにします。

    このオプションには、証明書内のすべての証明書チェーンが含まれています。

    c. [Next] をクリックします。
19. パスワード ウィンドウで、**keystore** と入力し、確認のために再入力します。

    このパスワードは、IoT FND と TPS プロキシがこのファイルを読み取るために使用するデフォルトのパスワードです。
20. [Next] をクリックします。
21. [File to Export] ウィンドウに、ファイル名（*nms_cert* または *tps_cert* など）を入力し、[Next] をクリックします。
22. [Completing the Certificate Export Wizard] で、[Finish] をクリックします。

    *.pfx 拡張子を持つファイルは、デスクトップに自動的に保存されます。PFX とは、Personal Information Exchange 形式のことであり、PKCS_#12 形式とも呼ばれます。PFX は、コンピュータ間で証明書と秘密キーを転送（エクスポート）可能にするための、業界標準形式です。
23. 2 つの証明書ファイル（*nms_cert.pfx* および *tps_cert.pfx*）は、Windows デスクトップから IoT FND（*nms_cert.pfx*）および TPS プロキシ（*tps_cert.pfx*）にそれぞれ安全に転送されます。

    (注)セキュリティを向上させるには、転送が正常に実行されたら、*.pfx ファイルを Windows デスクトップから削除して、ごみ箱を空にします。

コマンド認可サポート

Cisco Connected Grid ルータ（CGR）は、3G、4G、または WiMAX などの WAN バックホール接続を介して IoT FND により管理されます。CG-OS CGR の場合、IoT FND に対する管理権限を有効にするには、OID 値を定義します。

このポリシーの OID は、1.3.6.1.4.1.9.21.3.3.1 です。IoT FND が管理権限で管理コマンドを CGR に対して発行することが許可されている場合に、この要素は表示されます。IoT FND は TLS などのセキュア セッションを介して CGR と通信し、CGR はそれらのコマンドを、ネットワーク管理者が発行したかのように実行できます。

ここでは、次の内容について説明します。

- NMS/TPS 証明書を使用したコマンド認可の有効化
- CA 証明書への OID 値の追加
- 証明書の更新

NMS/TPS 証明書を使用したコマンド認可の有効化

ルータのコマンド認可（CA）機能を承認するための手順に従い、IoT FND への登録を実行します。

1. 新しい NMS/TPS 証明書を生成するか（IoT FND および IoT FND TPS プロキシの証明書の生成を参照）、既存の NMS/TPS 証明書を更新します（証明書の更新を参照）。
2. OID 値を CA 証明書に追加します（CA 証明書への OID 値の追加を参照）。
3. NMS/TPS 証明書の新しい .pfx ファイルを生成します（IoT FND および IoT FND TPS プロキシの証明書の生成を参照）。
4. IoT FND を停止します（IoT FNDの停止を参照）。
5. 既存の cgms_keystore ファイルの名前を変更します（たとえば、cgms_keystore_no_oid）。
6. .pfx ファイルを IoT FND にエクスポートし、新しい cgms_keystore ファイルを作成します（キーツールを使用した cgms_keystore ファイルの作成を参照）。
7. 新しい証明書をインストールします（証明書のインストールを参照）。
8. 新しい cgms_keystore ファイルを IoT FND に追加します（cgms_keystore ファイルの IoT FND へのコピーを参照）。
9. IoT FND を開始します（IoT FND の起動を参照）。
10. ルータを IoT FND に登録します。

CA 証明書への OID 値の追加

IoT FND がルータ上でのコマンド認可に管理者役割を使用できるようにするには、OID 値を CA 証明書に追加する必要があります。

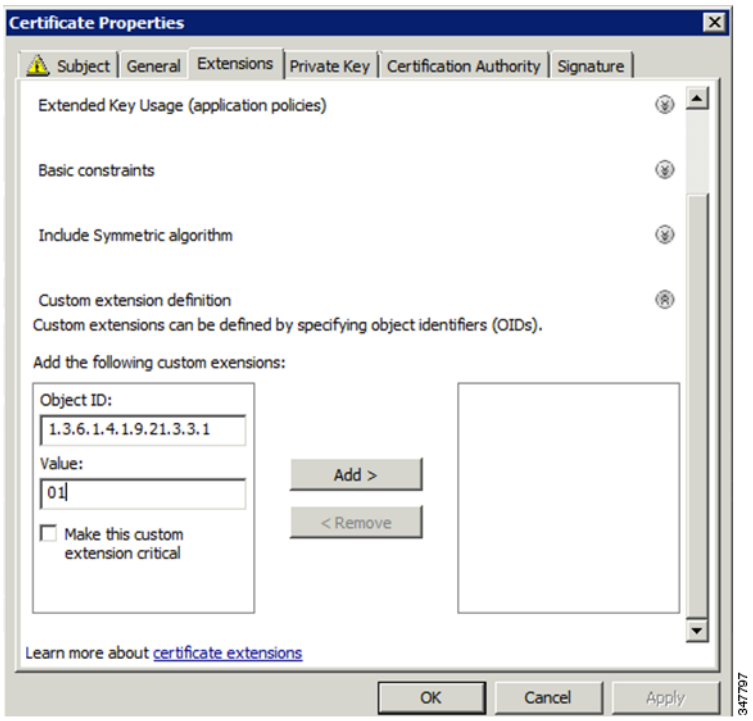
OID 値を CA 証明書に追加するには、次の手順を実行します。

1. CA サーバ上で、cmd コンソールを開き、次のように入力します。

```
certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
```

2. CA を再起動します。
3. [Select Certificate Enrollment Policy] ウィンドウで、[Active Directory Enrollment Policy] を選択し、[Next] を選択します。

4. [Request Certificates] ウィンドウで、次の手順を実行します。
   a. [NMS] チェックボックスをオンにします。
   b. [More information...] リンクをクリックします。
5. [Certificate Properties] ウィンドウで、[Subject] タブをクリックし、フィールドに入力します。
6. [Certificate Properties] ウィンドウで、[Extensions] タブをクリックし、[Custom extension definition] ボタンをクリックして、セクションを展開します。



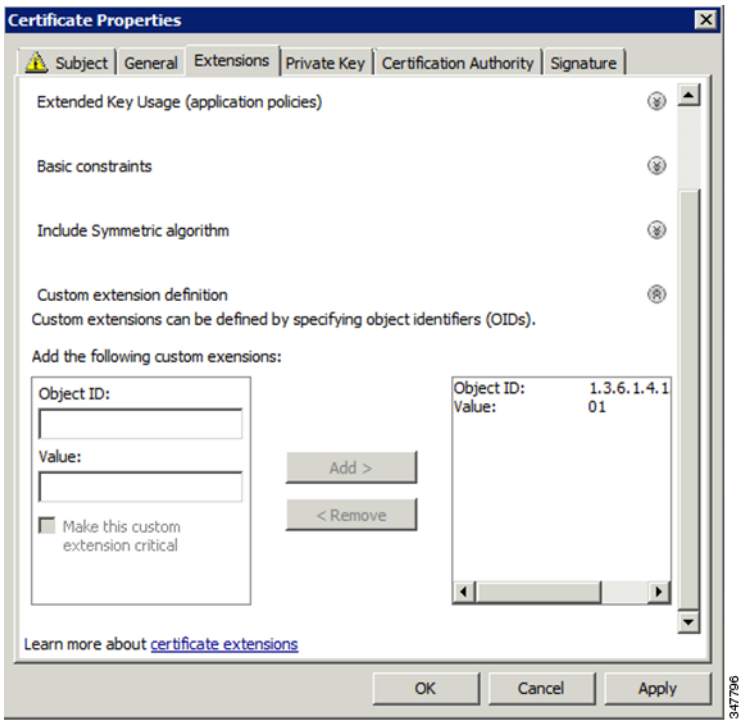
7. [Object ID] フィールドに、次のように入力します。

   ```
   1.3.6.1.4.1.9.21.3.3.1
   ```

8. [Value] フィールドに、次のように入力します。

   ```
   01
   ```

9. [Add] をクリックします。



OID と値は、カスタム拡張機能として右側のフィールドに追加されます。

10. これらの値が正しいことを確認し、[Apply] をクリックします。

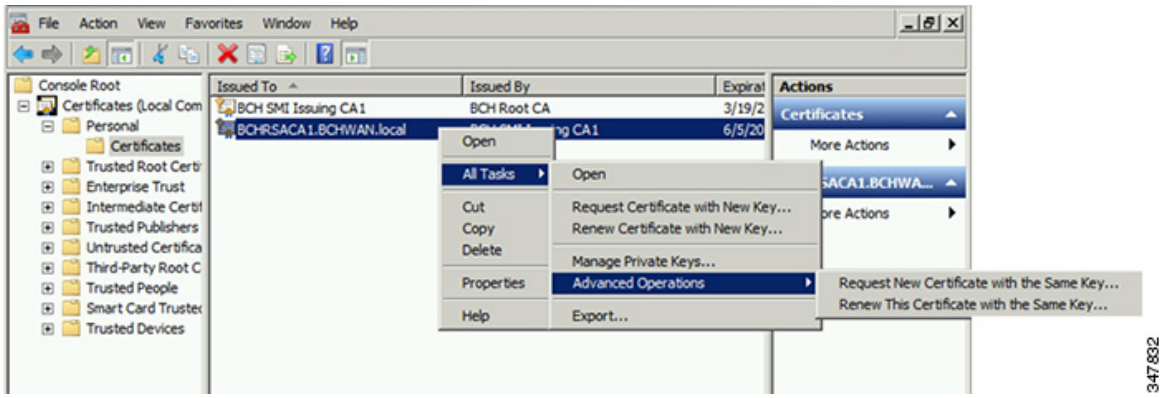
証明書の更新

証明書を更新し、OID 値を追加するには、次のようにします。

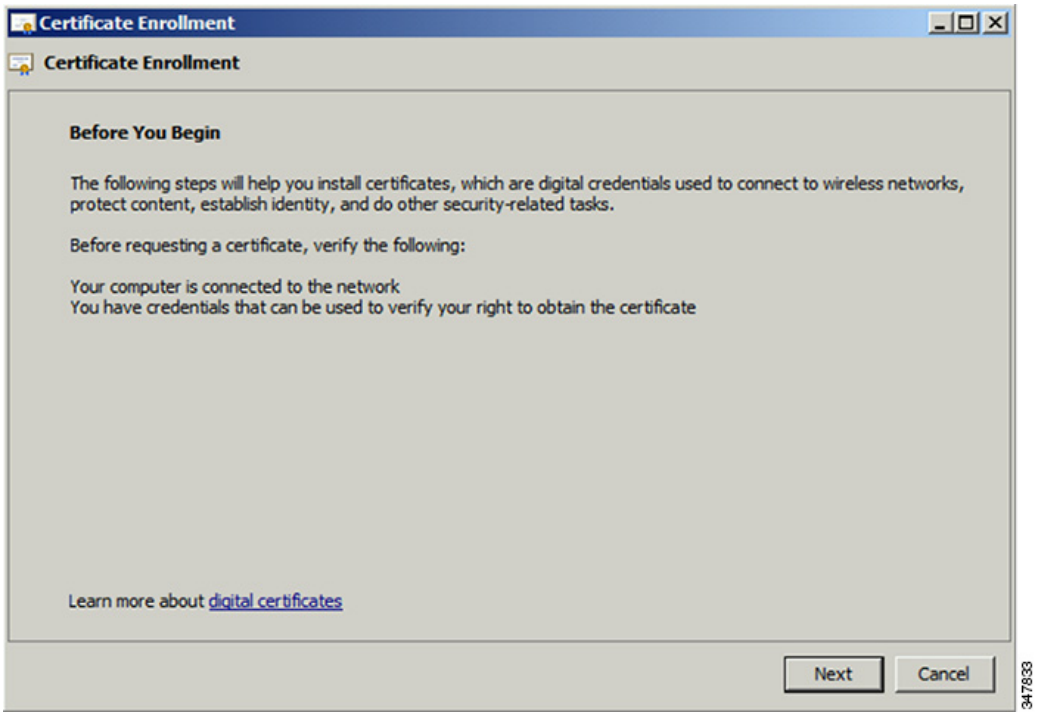
1. 元の NMS/TPS 証明書がある RSA CA サーバから、コマンド プロンプトで次のオープン コマンドを入力します。

   ```
   certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
   ```

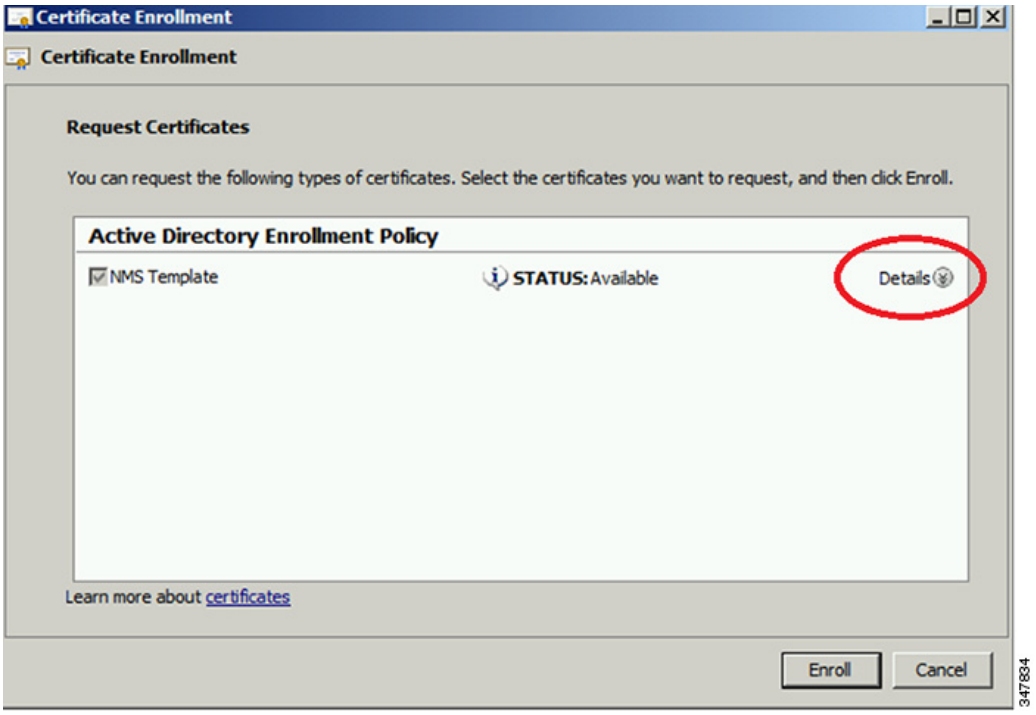
2. CA サーバを再起動します。
3. MMC で証明書のコンソールを開きます。
4. CA サーバ上の Personal フォルダ内から、発行された NMS/TPS 証明書を見つけます。
5. サーバ アイコンを右クリックし、コンテキスト メニューから [All Tasks] > [Advanced Operations] > [Renew This Certificate with the Same Key] オプションを選択します。



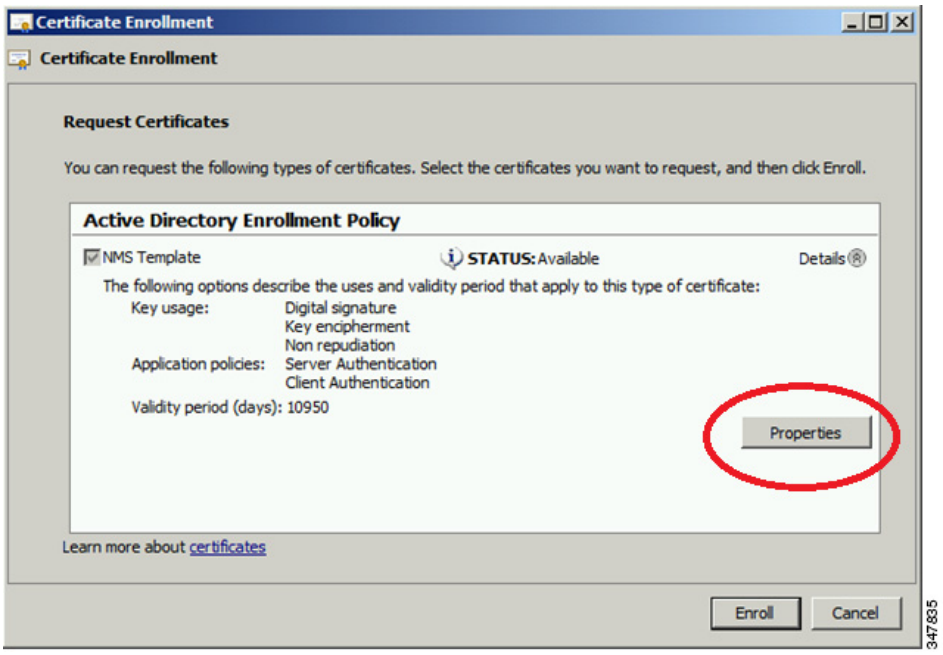
6. [Certificate Enrollment] ウィンドウで、[Next] をクリックします。



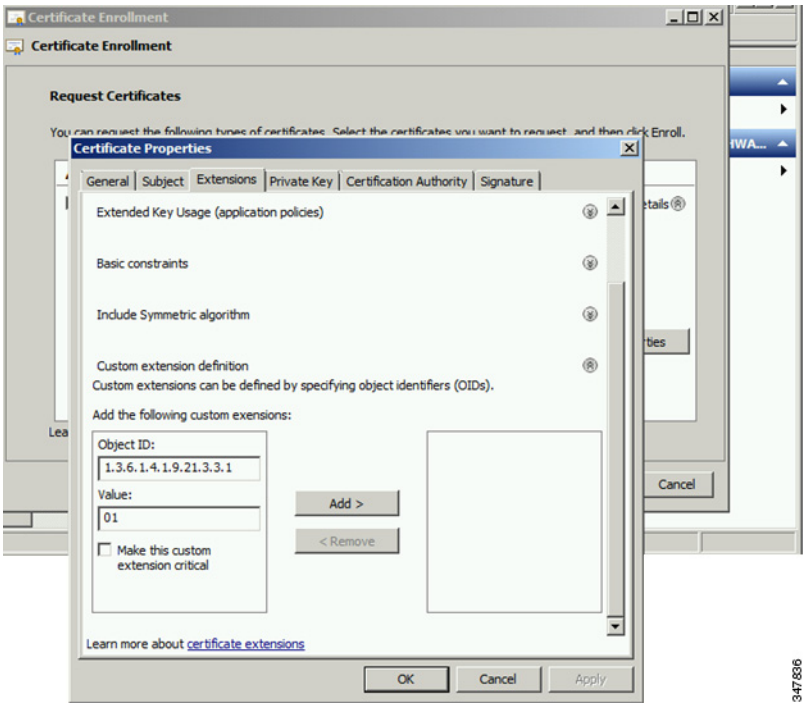
7. [Details] をクリックします。



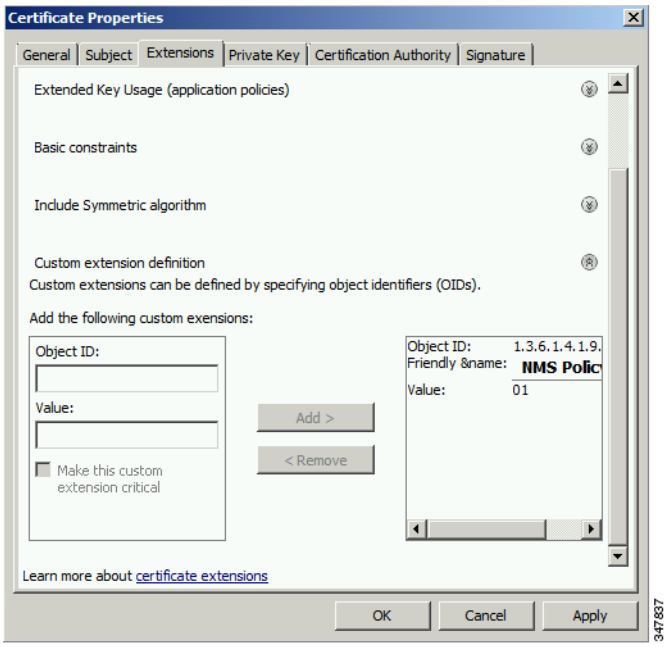
8. [Properties] をクリックします。



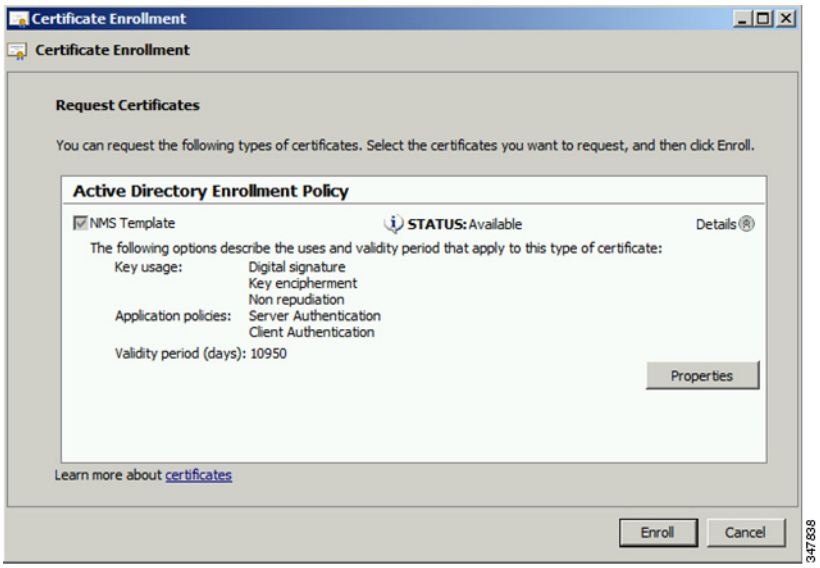
9. OID とその値を入力し、[OK] をクリックします。



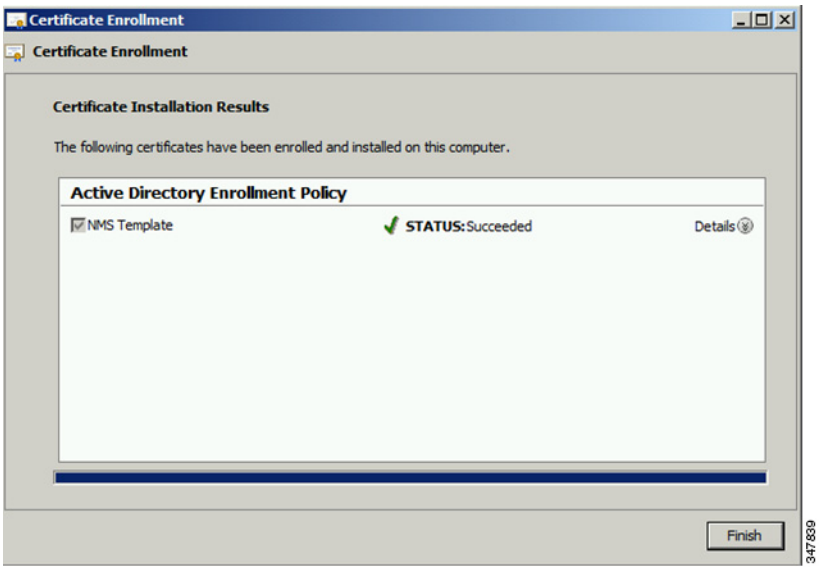
10. [Add>] をクリックし、次に [OK] をクリックします。



11. [Enroll] をクリックします。



12. [Finish] をクリックします。



13. 証明書に OID 値が含まれていることを確認します。

HSM のカスタム CA の設定

この項では、IoT FND からメッシュ デバイスに送信される CSMP メッセージに署名するための、ハードウェア セキュリティ モジュール（HSM）用のカスタム CA の設定について説明します。

はじめる前に

- 表 1（22 ページ） にリストされている SafeNet クライアント ソフトウェア バージョンが、IOT-FND サーバ上にインストールされていることを確認します。
- 独自の CA（たとえば、Microsoft や OpenSSL）を持つ必要があります。

HSM 証明書を生成するためのカスタム CA を設定するには、次の手順を実行します。

1. HSM 上に新しいパーティションを作成し、それを IoT FND クライアントに割り当てます(HSM クライアントの設定を参照)。
2. HSM 上でキーペアを生成し、そのキーペアの CSR をエクスポートします(キーストアを参照)。

   すべてのコマンドは、IoT FND サーバ上の Luna クライアントから実行します。HSM マシンにログインする必要はありません。

```
[root@<user>-scaledb bin]# cd /usr/safenet/lunaclient/bin/

# Generate a Key Pair (a set of private and public keys.You MUST provide explicit labels to the
private and public keys)
[root@<user>-scaledb bin]# ./cmu generatekeypair -sign=T -verify=T -labelpublic="nms_public_key"
-labelprivate="nms_private_key"
Please enter password for token in slot 1 : ********
Enter key type - [1] RSA  [2] DSA [3] ECDSA : 3    <--- Choose option 3
Enter curve type [1] NISTP 192
                 [2] NISTP 224
                 [3] NISTP 256
                 [4] NISTP 384
                 [5] NISTP 521

Enter curve type [1] NISTP 192
                 [2] NISTP 224
                 [3] NISTP 256   <--- Choose option 3
                 [4] NISTP 384
                 [5] NISTP 521
 (1 to 5) 3
[root@<user>-scaledb bin]#

# Test if the keypair exists on the HSM partition

[root@<user>-scaledb bin]# ./cmu list
Please enter password for token in slot 1 : ********
handle=2000001    label=nms_public_key
handle=2000002    label=nms_private_key

# Now, export a certificate signing request for this keypair.Note that the specific fields for DN
and handle may be different for your HSM.Fill appropriately.

[root@<user>-scaledb bin]#./cmu requestcertificate
Please enter password for token in slot 1 : ********
Select the private key for the request :

Handler    Label
2000002    nms_private_key
Enter handler (or 0 for exit) : 2000002
Enter Subject 2-letter Country Code (C) : US
Enter Subject State or Province Name (S) : CA
Enter Subject Locality Name (L) : San Jose
Enter Subject Organization Name (O) : Cisco Systems Inc.
Enter Subject Organization Unit Name (OU) : IOTSSG
Enter Subject Common Name (CN) : IOT-FND-HSM
Enter EMAIL Address (E) :
Enter output filename : hsm.csr
[root@<user>-scaledb bin]#

# Verify the file exists and has properly formatted content

[root@<user>-scaledb bin]# ls hsm.csr
hsm.csr
```

```
[root@<user>-scaledb bin]# cat hsm.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBKzCB0QIBADBvMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcT
CFNhbiBKb3NlMRowGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEluYzEPMA0GA1UECxMG
SW9UU1NHMRMwEQYDVQQDEwpDRy1OTVMtSFNNMFkwEwYHKoZIzj0CAQYIKoZIzj0D
AQcDQgAESfdlrrcVtzN3Yexj9trlI5qd0w5Sdu8Vj2s17JAF/vPFUOYIw/uXwD6+
bb8vq3WHlA6tmgRbj+FU6G3Bmt/vCqAAMAsGByqGSM49BAEFAANIADBFAiEAroJO
qz3dHA2GLrGzBmUO1vYys642Nkb4B4qyEoUZIGsCIFs0iTUyGQreM1BaSDEPHArZ
RvFlrKo/Zi3c8O4gzFZW
-----END NEW CERTIFICATE REQUEST-----
```

3. 生成された CSR を CA に保存して、証明書に署名します。

   (注) 証明書は必ず有効期限を 30 年として署名します。メッシュ ノードは、30 年未満の有効期限で署名された証明書はすべて拒否します。ノード アドミッションのための 802.1x 認証に使用されるルート CA を使用できます。

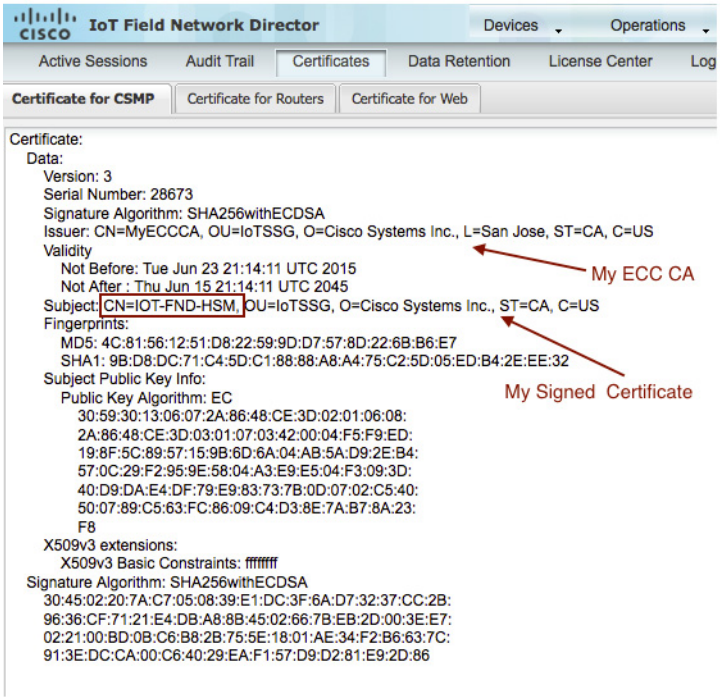
4. 署名付き証明書を IoT FND サーバにコピーして、HSM にインポートします。

```
[root@<user>-scaledb bin]# ./cmu import
Please enter password for token in slot 1 : ********
Enter input filename : <your file name with signed certificate>

# Verify that the certificate was imported

[root@<user>-scaledb bin]# ./cmu list
Please enter password for token in slot 1 : ********
handle=2000001    label=nms_public_key
handle=2000002    label=nms_private_key
handle=2000003    label=IOT-FND-HSM    <--- This is my certificate with label = CN
```

5. この新しい証明書を使用するように IoT FND を設定します。

```
[root@kartven2-nms ~]# service cgms stop
[root@kartven2-nms ~]# cd /opt/cgms/server/cgms/conf/

# Add following properties to the cgms.properties file

hsm-private-key-label=nms_private_key     <--- private key label you gave to your public key
hsm-public-key-label=nms_public_key       <--- public key label you gave to your public key
hsm-cert-label=IOT-FND-HSM                <--- label for your signed certificate
hsm-keystore-name=customca-group          <--- your HA partition group
hsm-keystore-password=2bVvZsq+vsq94YxuAKdaag==   <--- encrypted password for the partition

[root@kartven2-nms conf]# service cgms start
[root@kartven2-nms conf]#
```

6. 証明書が [Certificates for CSMP] タブに表示されることを確認します([Admin] > [Certificates])。



7. 署名にこの証明書を使用するように、メッシュ ノードを設定します。

SSM のカスタム CA の設定

この項では、IoT FND からメッシュ デバイスに送信される CSMP メッセージに署名するための、ソフトウェア セキュリティ モジュール(SSM)用のカスタム CA の設定について説明します。

はじめる前に

- 表 1(22 ページ) にリストされている SafeNet クライアント ソフトウェア バージョンが、IOT-FND サーバ上にインストールされていることを確認します。
- サポート対象は、SSM バージョン 2.2.0-37 以上です。
- 独自の CA(たとえば、Microsoft や OpenSSL)を持つ必要があります。

SSM 証明書を生成するためのカスタム CA を設定するには、次の手順を実行します。

1. ssm サービスを停止します。

```
[root@nms-rhel-6-6 ~]# stop ssm
```

2. ssm_setup.sh スクリプトを使用して、新しいキーペアを特定のエイリアスで設定し、CSR を生成します。

```
[root@nms-rhel-6-6 ~]# cd /opt/cgms-ssm/bin/
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP   <--- Choose option 2

3.Import a trusted certificate
```

```
4.Change CSMP keystore password

5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit


Enter your choice : 2
Warning: This action will modify ssm_csmp_keystore file.Backup the file before performing this
action.
Do you want to proceed (y/n): y

Enter current ssm_csmp_keystore password :
Enter a new key alias name (8-16): ssmcustomca
Enter key password (8-12):

Enter certificate issuer details

Enter common name CN [Unknown]: IOT-FND-SSM

Enter organizational unit name OU [Unknown]: IOTSSG

Enter organization name O [Unknown]: Cisco Systems Inc.

Enter city or locality name L [Unknown]: San Jose

Enter state or province name ST [Unknown]: CA

Enter country code for this unit C [Unknown]: US


Is [CN=IOT-FND-SSM, OU=IOTSSG, O=Cisco Systems Inc., L=San Jose, ST=CA, C=US] correct (y/n)? :y
Certificate Signing Request file name: /opt/ssmcustomca.csr
Succefully generated keypair with alias ssmcustomca.You can use the CSR from /opt/ssmcustomca.csr
for signature by certificate authority
[root@nms-rhel-6-6 bin]#
```

3. 生成された CSR を CA に保存して、証明書に署名します。

   (注) 証明書は必ず有効期限を 30 年として署名します。メッシュ ノードは、30 年未満の有効期限で署名された証明書はすべて拒否します。ノード アドミッションのための 802.1x 認証に使用されるルート CA を使用できます。

4. 署名付き証明書を IoT FND サーバにコピーして、SSM にインポートします。

5. ssm_setup.sh スクリプトを使用して、2 つの証明書を SSM キーストアにインポートします。

```
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP

3.Import a trusted certificate   <--- Choose option 3

4.Change CSMP keystore password
```

```
5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit


Enter your choice : 3

Enter current ssm_csmp_keystore password :
Enter the alias for import: root
Certificate file name: /opt/ca.crt
Certificate reply was installed in keystore
Succefully imported certificate into alias root
```

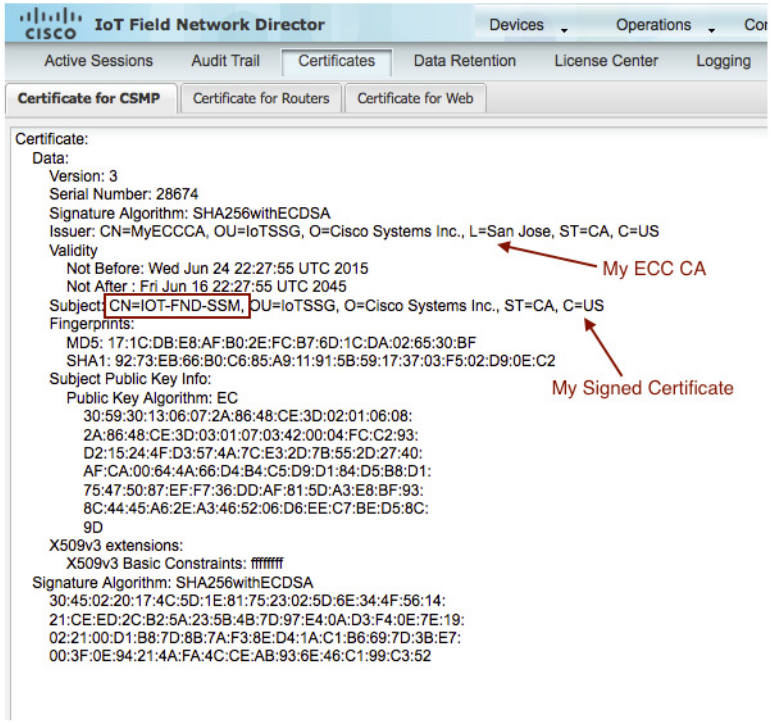
6. ssm_setup.sh スクリプトを使用して、エイリアスの署名付き証明書認証をインポートします。

```
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP

3.Import a trusted certificate   <--- Choose option 3

4.Change CSMP keystore password

5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit


Enter your choice : 3

Enter current ssm_csmp_keystore password :
Enter the alias for import: ssmcustomca
Certificate file name: /opt/ssmcustomca.crt
Certificate reply was installed in keystore
Succefully imported certificate into alias ssmcustomca
```

7. cgms.properties ファイルを次のパラメータで更新して、IoT FND がこの証明書を署名のために SSM で使用するように設定します。

```
security-module=ssm
ssm-host=172.27.163.153
ssm-port=8445
ssm-keystore-alias=ssmcustomca
ssm-keystore-password=GgeQJAOk3fSIH97qJARGRA==
ssm-key-password=GgeQJAOk3fSIH97qJARGRA==
```

8. 証明書が [Certificates for CSMP] タブに表示されることを確認します（[Admin] > [Certificates]）。



9. 署名にこの証明書を使用するように、メッシュ ノードを設定します。

CA 証明書のエクスポート

証明書を認証局または下位 CA から IoT FND にエクスポートするには、次の手順を実行します。

1. Windows Server 2008 R2 Enterprise エディションを稼働するシステム上で、認証局アプリケーションを開きます。
2. メニューを展開して、[Certificates (Local Computer)] > [Personal] > [Certificates] フォルダを表示します。
3. フィンガープリントが Cisco CGR 1000 と Cisco ASR により使用されているものと一致する証明書を見つけます。
4. 証明書を右クリックして、コンテキスト メニューから [All Tasks] > [Export] を選択します。
5. [Certificate Export Wizard] ウィンドウで、[Next] をクリックします。
6. [Export Private Key] ウィンドウで、[No, do not export the private key] ラジオ ボタンを選択します。[Next] をクリックします。
7. [Export File Format] ウィンドウで、[Base-64 encoded X.509（.CER）] ラジオ ボタンをオンにします。[Next] をクリックします。
8. [File to Export] ウィンドウで、エクスポートするファイルに名前を割り当てます。[Next] をクリックします。
9. [File to Export] ウィンドウに、ファイル名（*ca_cert* または *subca_cert* など）を入力し、[Next] をクリックします。
10. [Completing the Certificate Export Wizard] で、[Finish] をクリックします。

*.cer 拡張子を持つファイルは、デスクトップに自動的に保存されます。

11. 証明書ファイル(*ca_cert.cer* など)を、Windows デスクトップから IoT FND に安全に転送します。

(注)セキュリティを向上させるには、転送が正常に実行されたら、*.cer ファイルを Windows デスクトップから削除して、ごみ箱を空にします。

証明書のインストール

cgms_keystore ファイルは、IoT FND と IoT FND TPS プロキシを稼働している両方のサーバ上に作成する必要があります。

- **IoT FND**:cgms_keystore ファイルを作成するときは、IoT FND 証明書、秘密キー、および証明書チェーンをインポートする必要があります。cgms_keystore ファイルを作成したら、それをサーバ上の特定のディレクトリにコピーします。
- **IoT FND TPS プロキシ**:cgms_keystore ファイルを作成したら、IoT FND TPS プロキシの証明書、秘密キー、および証明書チェーンをインポートします。cgms_keystore ファイルを作成したら、TPS プロキシ上の特定のディレクトリにそれをコピーします。

TPS プロキシおよび IoT FND 用の cgms_keystore を作成するには、キーツールを使用して、次の手順を実行します。

はじめる前に

- キーストアに使用するパスワードを決定します。

  この章の例では、このパスワードを *keystore_password* としています。

キーツールを使用した cgms_keystore ファイルの作成

IoT FND と TPS プロキシの両方に対して cgms_keystore ファイルを作成するには、次の手順を実行します。

1. root として、.pfx ファイルの内容を、サーバ上(IoT FND および TPS プロキシ)で次のコマンドを入力して表示します。

[root@*tps_server* ~]# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12

(注).pfx の内容を表示すると、インポート時に必要なエイリアス名を入手できます。

2. プロンプトが表示されたら、キーストアのパスワードを入力します。

これは、.pfx ファイルの作成時に入力したものと同じパスワードです。

表示される情報には(次の例を参照)、3. に必要な alias_name が含まれています。

3. 証明書を cgms_keystore ファイルにインポートするには、次のコマンドを入力します。

```
keytool -importkeystore -v -srckeystore filename.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias alias_name -destalias cgms
-destkeypass
keystore_password
```

4. プロンプトで、宛先キーストア パスワードを入力します。
5. プロンプトが表示されたら、キーストアのパスワードを再入力します。
6. ソースのキーストア パスワードの入力を求めるプロンプトが表示されたら、.pfx ファイルの作成時に使用したパスワードを入力します(*nms_cert.pfx* または *tps_cert.pfx* のどちらか)。

(注) この例では、**keystore** が *.pfx* ファイルを作成したときのパスワードです。

例

nms_cert.pfx ファイルを表示して別名にアクセスするには、root として以下のコマンドを入力します。

(注) この例は、*nms_cert.pfx* についての手順を示しています。*tps_cert.pfx* に関する詳細を表示して、証明書を TPS プロキシにインポートするには、同じコマンドを使用しますが、*nms_cert.pfx* の部分は *tps_cert.pfx* に置き換え、*tps_cert.pfx* ファイルからの別名を使用します。

```
# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12
Enter keystore password: keystore
Keystore type: PKCS12
Keystone provider: SunJSSE
Your keystore contains 1 entry
Alias name: le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b
Creation date: March 29.2012
Entry type: PrivateKey Entry
Certificate chain length: 3
Certificate[1]:
Owner: CN=nms.sgbu.cisco.com
Issuer: CN=cisco-RSA-SUBCA-CA, DC=cisco, DC=com
...
```

証明書を IoT FND 上の **cgms_keystore** ファイルにインポートするには、root として次のコマンドを入力します。

```
# keytool -importkeystore -v -srckeystore nms_cert.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias
le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b -destalias cgms
-destkeypass
keystore_password

Enter destination keystore password: keystore_password
Re-enter new password: keystore_password
Enter source keystore password: keystore
...Storing cgms_keystore
```

(注) ***cgms*_keystore** テキストが**保存**されたことは正常な完了を示します。

cgms_keystore ファイルの IoT FND へのコピー

cgms_keystore ファイルを次の IoT FND および TPS プロキシのディレクトリにコピーします。

1. IoT FND の場合は、cgms_keystore ファイルをディレクトリ **/opt/cgms/server/cgms/conf/** にコピーします。
2. TPS プロキシの場合、cgms_keystore ファイルをディレクトリ **/opt/cgms-tpsproxy/conf/** にコピーします。

(注) 証明書をアクティブで適用可能なものとするには、正しいディレクトリに入れておく必要があります。

CA 証明書のインポート

NMS 証明書のインポートに加え、CA(または subCA)証明書を cgms_keystore にインポートする必要があります。

CA 証明書を cgms_keystore にインポートするには、次の手順を実行します。

1. IoT FND アプリケーション サーバ上で、root としてログインします。
2. cgms_keystore ファイルが置かれている /opt/cgms/server/cgms/conf ディレクトリに移動します。

```
# cd /opt/cgms/server/cgms/conf
```

3. CA 証明書をインポートします。

```
# keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer
```

画面にスクリプトが表示されます。

4. プロンプトが表示されたら、キーストアのパスワードを入力します。
5. パスワードを再入力します。
6. 証明書を信頼するかどうかを確認するメッセージが表示されたら、**yes** と入力します。

証明書はキーストアに追加されます。

例

CA 証明書をインポートするには、次のコマンドを root として入力します。

```
# keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer
Enter keystore password: keystore_password
Owner:  CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Issuer: CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Serial number:50adbd57e6b136984f9c1512a0eb7174
Valid from: Wed Jan 11 10:58:09 PDT 2012 until: Wed Jan 11:08:59 PDT 2016
Certificate _fingerprints:
    MD5: AE:5D:F4:0A:2B:E5:C8:D8:4A:F4:18:56:FD:A7:8D:7D
    SHA1: 83:22:12:8C:6A:23:D3:08:2B:00:55:EF:BD:FF:BA:47:97:99:7E:41
    Signature algorithm name: SHA1withRSA
    Version:3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
#2:ObjectId: 2.5.29.15 Criticality=false
KeyUsage[
DigitalSignature
Key_CertSign
Crl_Sign
]
#3:ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000:C6 AB 38 CC EE 79 B0 51 3B 4D 13 c8 9A 56 F6 73 ..8..y.Q;M...V.s
0010:B9 19 FF 7B                                     ....
]
]
#4: ObjectId:1.3.6.1.4.1.311.21.1 Criticality=false
Trust this certificate [no] yes
Certificate was added to the keystore.
```

IoT FND TPS プロキシ キーストアへの CA 証明書のインポート

CA 証明書のインポート と同じ手順に従って、CA 証明書を IoT FND TPS プロキシ上の cgms_keystore にインポートします。

カスタム ブラウザ証明書のインストール

デフォルトの IoT FND インストール システムは、クライアント Web ブラウザまたは NB API クライアントのいずれかを使用する HTTP(S)通信に、自己署名証明書を使用します。必要であれば、ユーザ自身の CA サーバによって署名された証明書を使用できます。この項では、これらのカスタム証明書のインストール方法を示します。

この項では、次のトピックについて取り上げます。

- ブラウザ クライアントでのカスタム証明書のインストール
- North Bound API クライアント（Windows）を使用している場合のカスタム証明書のインポート
- Window IE を使用している場合のカスタム証明書のインポート
- カスタム証明書の管理
- North Bound API イベントの管理

はじめる前に

- クライアント ブラウザのキャッシュをクリアします。
- クライアント ブラウザで、NMS サーバの既存の証明書を（IP および DNS により）削除します。

  たとえば、Firefox では、[Preferences] > [Advanced] > [Encryption] > [View Certifications] を選択します。それぞれのサーバについてリスト内の証明書を削除します。
- 署名付き証明書で使用する共通名を選択します。

  この名前には、NMS サーバの IP アドレスに解決するための DNS エントリが必要です。
- 新しい証明書を生成し、それを .PFX ファイルにエクスポートします。

  このファイルには、秘密キー、パブリック証明書、および CA サーバ証明書が含まれている必要があります。

  cgms_keystore ファイルの秘密キーと公開キーを生成してそれらを .PFX ファイルにエクスポートする手順については、キーツールを使用した cgms_keystore ファイルの作成を参照してください。

ブラウザ クライアントでのカスタム証明書のインストール

1. NMS サーバで、既存の jbossas.keystore および jbossas.keystore.password ファイルを、/opt/cgms/server/cgms/conf/ ディレクトリから安全な場所にコピーします。
2. 既存の jbossas.keystore および jbossas.keystore.password ファイルを /opt/cgms/server/cgms/conf/ ディレクトリから削除します。
3. jbossas.keystore ファイルにインポートする予定の別名を、.PFX ファイル内で確認します。

   ```
   #keytool -list -v -keystore newcert.pfx -storetype pkcs12
   ```

   次のキーストア パスワードを入力します。***keystore_password_when_pfx_file_was_created***

   ```
   Keystore type: PKCS12
   Keystore provider: SunJSSE

   Your keystore contains 1 entry

   Alias name: le-nms-a88ef13a-a519-457f-a2e1-0540f5453ee0
   Creation date: Feb 23, 2016
   Entry type: PrivateKeyEntry
   Certificate chain length: 2
   Certificate[1]:
   …
   ```

4. .pfx ファイル形式の新しいカスタム証明書を新しい jbossas.keystore ファイルにインポートし、同時にエイリアス名を **jboss** に変更します。プロンプトに従います。

```
# keytool -importkeystore -v -srckeystore newcert.pfx -srcstoretype pkcs12
-destkeystore /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks-
srcalias le-nms-a88ef13a-a519-457f-a2e1-0540f5453ee0 -destalias
jboss -destkeypass your_keystore_password
Enter destination keystore password: your_keystore_password
Enter source keystore password: keystore_password_when_pfx_file_was_created
[Storing /opt/cgms/server/cgms/conf/jbossas.keystore]
```

5. （任意）SALT を定義します。

   （注）SALT を変更しない場合は、この手順をスキップすることができます。

   SALT は暗号化パスワードの強度を定義します。それは少なくとも 8 文字の長さにする必要があります。
   例：A1a1B2b2C3c3D4dE5e5F6f6G7g7H8h8I9i9J10j10K11k11L12l12M13m13N14n14O15

   a. ファイル /opt/cgms/server/cgms/deploy/security-service.xml を安全な場所にコピーします。

   b. /opt/cgms/server/cgms/deploy/security-service.xml ファイル内で SALT を更新します。

（注）実行している NMS リリースに応じて、手順 6 *または*手順 7 *のどちらか*を選択します。

6. **2.1.0 より *前の* CG-NMS リリース**では、キーストア パスワードは、ファイル /opt/cgms/server/cgms/conf/jbossas.keystore.password に保存します。

   この手順では、jbossas.keystore.password ファイルに保存されるパスワードを暗号化します。

   このパスワードは、手順 4. でインポートされた新しいカスタム証明書がある jbossas.keystore を開くために使用されます。

   a. /opt/cgms/bin/encrypt-password.sh スクリプトを、次のパラメータを指定して実行します。

   – 手順 5. で定義した新しい SALT を指定するか、または /opt/cgms/server/cgms/deploy/security-service.xml ファイル内にある既存のものを使用します。

   – count を 1024 に設定します。

   – パスワード ファイルを jbossas.keystore.password に設定します。

   – your_keystore_password を設定します。

```
#./encrypt-password.sh
A1a1B2b2C3c3D4dE5e5F6f6G7g7H8h8I9i9J10j10K11k11L12l12M13m13N14n14O15 1024 jbossas.keystore.password
your_keystore_password
```

   b. jbossas.keystore.password を /opt/cgms/server/cgms/conf ディレクトリに移動させるかまたはコピーします。

   c. ステップ 8 に進みます。

7. **2.1.0 または IoT FND 3.0 *以降の* CG-NMS リリース**では、キーストア パスワードはファイル /opt/cgms/server/cgms/conf/VAULT.dat に保存します。

   続く手順を実行し、パスワードを更新して、手順 4 で入力したもの（***your_keystore_password***）と一致するようにします。

   a. /opt/cgms/server/cgms/conf 内の VAULT.dat と vault.keystore ファイルを安全な場所にバックアップします。

   b. VAULT.dat ファイルを新しいパスワードで更新します。

```
#/opt/cgms/bin/vault.sh -k /opt/cgms/server/cgms/conf/vault.keystore -p cgms123
-e /opt/cgms/server/cgms/conf -i 50 -s 12345678 -v vault -b keystore_pass
-a password -x your_keystore_password
```

ここで、vault.keystore には VAULT.dat への参照が含まれており、VAULT.dat は jboss キーストア パスワードを保存して非表示にします。このコマンドは、新しい jboss.keytsore を含む新しい VAULT.dat ファイルを作成します。vault.keystore を開くデフォルトのパスワードは cgnms123 です。

8. IoT FND を再起動します。

```
# service cgms restart
```

9. ブラウザを使用して、NMS サーバに接続します。
10. 新しい証明書を承認し、追加します。
11. ブラウザを使用して IoT FND にログインします。

North Bound API クライアント(Windows)を使用している場合のカスタム証明書のインポート

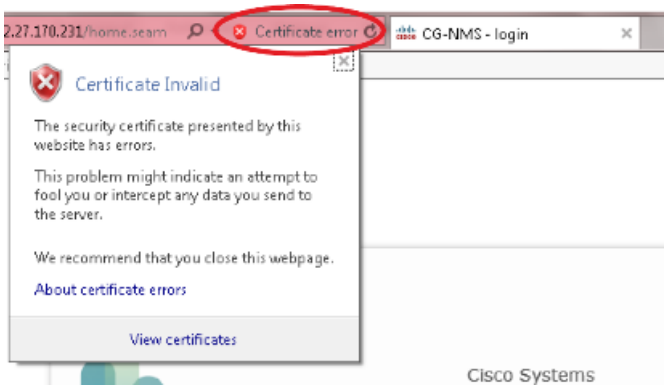
Windows Server 上で実行する NB API クライアントの場合は、CA パブリック証明書をローカル コンピュータ上の証明書ストアにインポートします。一致する CA パブリック証明書により、クライアント マシンは必ず NB API クライアントを使用して IoT FND と通信します。

Window IE を使用している場合のカスタム証明書のインポート

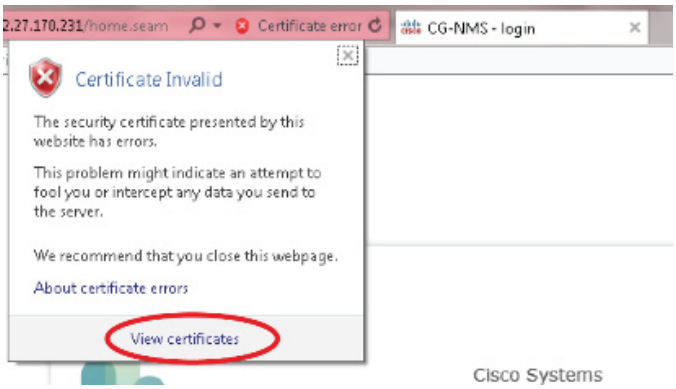
1. IE では、NMS サーバの https URL アドレスを入力します。

   URL 名は、NMS サーバ証明書の共通名と一致している必要があります。

2. [Security Alert] ウィンドウで、[OK] をクリックします。
3. [Security Certificate Warning] ウィンドウで、[Continue to this Website (Not Recommended)] リンクをクリックします。
4. [Security Alert] ウィンドウで、[OK] をクリックします。
5. アドレス バーの [Certificate error] セクションをクリックします。

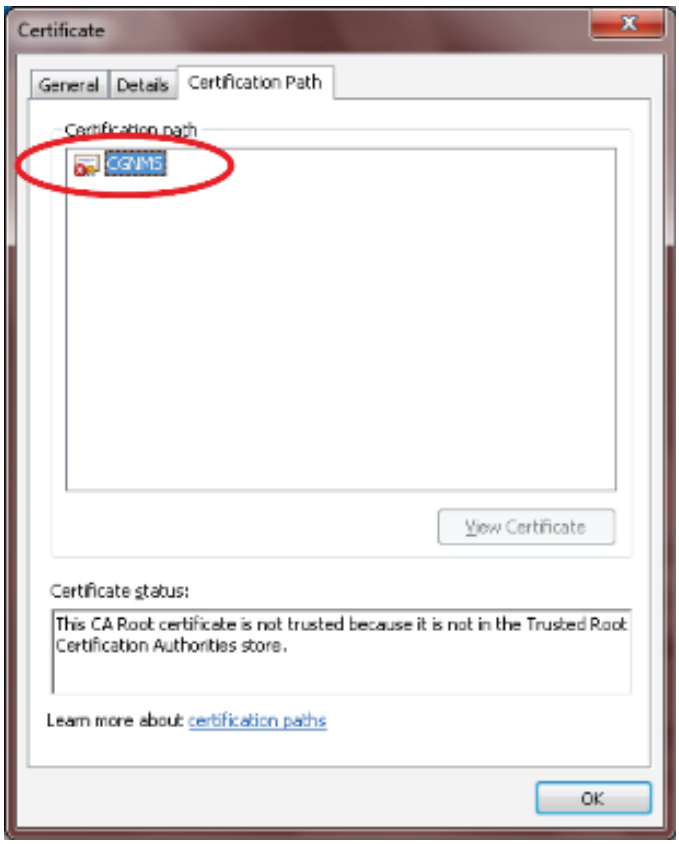


6. [Certificate Invalid] ウィンドウで、[View certificates] をクリックします。

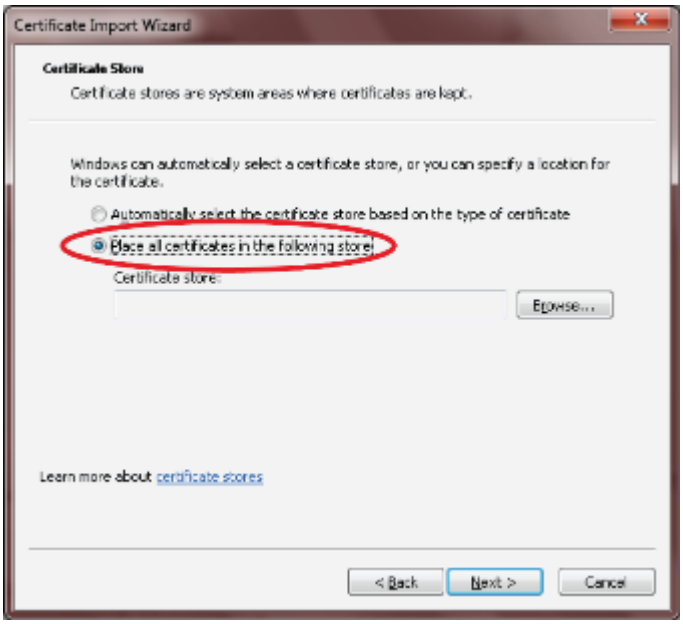


[Certificate] ウィンドウには、NMS サーバに対して発行され、発行元 CA（または下部 CA）サーバによって署名されたデバイス証明書がリストされます。

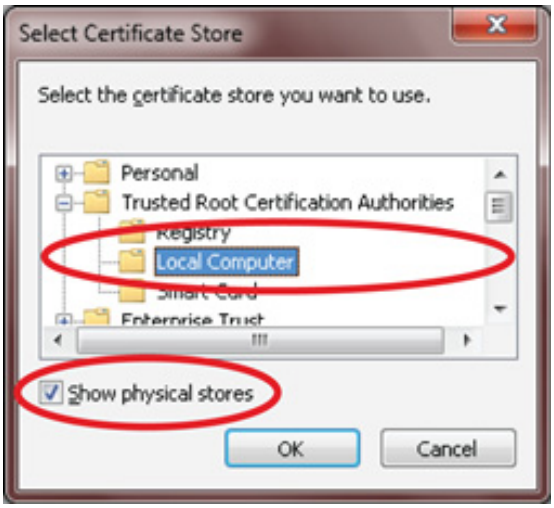
7. [Certification Path] タブを選択し、無効な証明書（つまり赤いバツ印が付いているもの）を探します。



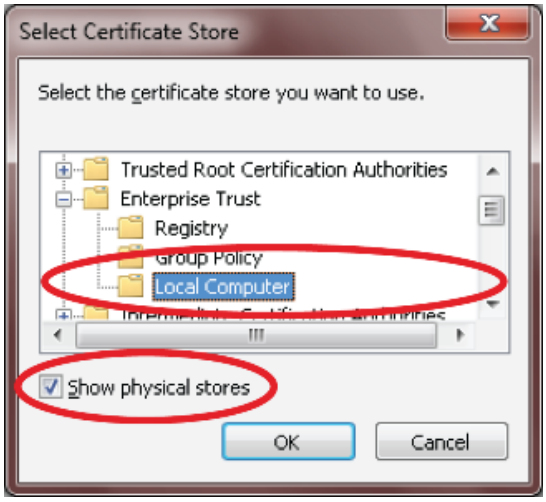
8. 無効な証明書を選択し、[General] タブを選択します。
9. [Install Certificate] をクリックします。
10. [Certificate Install Wizard] ウィンドウで、[Next] をクリックします。
11. [Place all certificates in the Following Store] を選択し、[Browse] をクリックします。



12. [Certificate Store] ウィンドウで、[Show physical stores] チェックボックスをオンにし、Trusted Root Certification Authorities フォルダを開き、[Local Computer] を選択して、[OK] をクリックします。



13. [Next] をクリックします。
14. [Finish] をクリックします。
15. [OK] をクリックします。
16. [Certificate] ウィンドウで、[Install Certificate] をクリックします。
17. [Place all certificates in the Following Store] を選択し、[Browse] をクリックします。
18. [Certificate Store] ウィンドウで、[Show physical stores] チェックボックスをオンにし、Trusted Root Certification Authorities フォルダを開き、[Local Computer] を選択して、[OK] をクリックします。



19. [Next] をクリックします。
20. [Finish] をクリックします。
21. [OK] をクリックします。
22. [Certificate] ウィンドウで、[OK] をクリックします。
23. アドレス バーの [Certificate error] セクションが引き続き表示される場合は、前述の手順を繰り返します。
    - NMS サーバに対して発行され、発行元 CA（または下部 CA）サーバによって署名されたデバイス証明書が、[Certificate] ウィンドウに表示されていることを確認します。
    - [Certification Path] タブを選択し、パス内のすべての証明書が有効である（つまり、証明書の上に赤いバツ印が付いていない）ことを確認します。
24. ブラウザを閉じてから再起動します。
25. アドレス バーに、IoT FND サーバのセキュア URL を入力します。

    IoT FND ログイン ページが表示されます（セキュリティ画面は表示されません）。

カスタム証明書の管理

1. IoT FND を更新するかまたはフレッシュ インストールを実行するときに上書きされる次のファイルをバックアップします。
    - /opt/cgms/server/cgms/conf/ ディレクトリ内の次のファイル：
        - jbossas.keystore.password
        - jbossas.keystore
    - /opt/cgms/server/cgms/deploy/ ディレクトリ内の次のファイル：
        - security-service.xml ファイル

        これは、ブラウザ クライアントでのカスタム証明書のインストールで SALT 値を追加したファイルです。
    - /opt/cgms/server/cgms/conf ディレクトリ内の次のファイル：
        - VAULT.dat
        - vault.keystore

2. IoT FND のアップグレードまたは新規インストールを実行します（IoT FND のアップグレードを参照）。
3. 上記のファイルをそれぞれの該当するフォルダにコピーして、IoT FND を再起動します。

North Bound API イベントの管理

North Bound（NB）API クライアントは、HTTPS を使用してイベントを送信できます。NB API クライアントは、IoT FND がイベント送信に使用する有効な URL HTTPS を提供することで、IoT FND をサブスクライブする必要があります。IoT FND は、NB API クライアントがパブリッシュする SSL 証明書とハンドシェイクを受け入れます。

キーストアにアクセスするための IoT FND の設定

cgms_keystore を作成し、NMS と CA 証明書をそれにインポートしたら、IoT FND が cgms_keystore ファイルにアクセスするように設定します。

keystore パスワードを設定するには、次の手順を実行します。

1. IoT FND を停止します。
2. setupCgms.sh スクリプトを実行します。

```
pwd
/opt/cgms/bin
./setupCgms.sh
06-12-2012 10:21:39 PDT: INFO: ========== CG-NMS Setup Started - 2012-06-12-10-21-39 =====
06-12-2012 10:21:39 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log
Are you sure you want to setup CG-NMS (y/n)? y
06-12-2012 10:21:39 PDT: INFO: User response: y
...
Do you want to change the keystore password (y/n)? y
06-12-2012 10:21:52 PDT: INFO: User response: y
Enter keystore password: keystore_password
Re-enter keystore password: keystore_password
06-12-2012 10:21:59 PDT: INFO: Configuring keystore password.This may take a while.
Please wait ...
06-12-2012 10:22:00 PDT: INFO: Keystore password configured.
...
```

このスクリプトは、cgms.properties ファイル内に設定されたパスワードを保存します。

3. IoT FNDを起動します。

ヒント：cgms_keystore と cgms.properties ファイルを保護するには、そのアクセス許可を root の読み取り専用に設定します。

注意：システムは必ず保護してください。root でのみ IoT FND サーバにアクセスできることを確認します。ファイアウォールは必ず内部ホストからの SSH アクセスのみを許可するように設定します。

キーストアにアクセスする TPS プロキシの設定

keystore にアクセスするように TPS プロキシを設定するには、次のようにします。

1. tpsproxy bin ディレクトリに移動します。

```
cd /opt/cgms-tpsproxy/bin
```

2. 選択したパスワードを暗号化形式に変換します。

```
./encryptionUtil.sh {your chosen password for cgms_keystore}
7jlXPniVpMvat+TrDWqh1w==
```

3. 暗号化したパスワードを tpsproxy.properties ファイルにコピーします。

   a. 編集のためにファイルを開きます。

   ```
   cd /opt/cgms-tpsproxy/conf
   emacs tpsproxy.properties
   ```

   b. ファイルに次の行を追加します。

   ```
   cgms-keystore-password-hidden=keystore_password
   ```

   この例では、暗号化された *keystore_password* は「7jlXPniVpMvat+TrDWqh1w==」です。

4. TPS プロキシを再起動します。

```
service tpsproxy restart
```

HSM クライアントの設定

HSM クライアントをセットアップするには、次の手順を実行します。

- IoT FND サーバ上への HSM クライアントのインストール
- HSM HA クライアントの設定

(注)インストール システムで CSMP ベースのメッセージングに SSM を使用している場合は、SSM のインストールと設定を参照してください。

IoT FND サーバ上への HSM クライアントのインストール

ハードウェア セキュリティ モジュール(HSM)は、ポート 1792 でリスニングするセキュリティ サーバとして機能します。IoT FND が HSM と通信するようにセットアップするには、次の手順を実行します。

1. HSM クライアントを IoT FND サーバ上にインストールします。
2. HSM クライアントが HSM の証明書を持つように設定します。
3. 証明書を HSM にアップロードします。

この項では、HSM クライアントをインストールして設定する方法を説明していますが、HSM は 172.16.0.1、クライアントは 172.31.255.254 であると想定しています。

HSM クライアントをインストールしてセットアップするには、次の手順を実行します。

1. HSM クライアント パッケージを取得して、アンパックし、インストール スクリプトを実行します。

   ```
   sh install.sh
   ```

2. /usr/lunasa/bin ディレクトリに移動します。

   ```
   cd /usr/safenet/lunaclient/bin/
   ```

3. クライアント証明書を作成します。

   ```
   ./vtl createCert -n ip_address_of_hsm_client
   ```

4. HSM サーバから HSM 証明書をダウンロードします。

   ```
   scp admin@ip_address_of_hsm_server:server.pem .
   ```

5. クライアント証明書を HSM サーバにアップロードします。

```
scp ../cert/client/ip_address_of_hsm_client.pem admin@ip_address_of_hsm_server: .
```

6. HSM 証明書をロードします。

```
vtl addServer -n ip_address_of_hsm_server -c server.pem .
```

7. HSM サーバが追加されていることを確認します。

```
vtl listServer
```

8. HSM クライアントから、SSH を使用して HSM サーバにログインします。

```
ssh admin@ip_address_of_hsm_server
Last login: Mon Aug 15 15:36:43 2012 from 10.27.164.171
Luna SA 5.0.1-2 Command Line Shell - Copyright (c) 2001-2010 SafeNet, Inc. All rights reserved.
[TestLunaSA1] lunash:>
```

9. SSH を使用して、HSM サーバ上で次の手順を実行します。

   a. クライアントを HSM サーバに追加します。

```
[TestLunaSA1] lunash:>client register -c hsm_client_name -i ip_address_of_hsm_client
'client register' successful.     Command Result : 0 (Success)
```

   b. 次の手順で、サーバ上で定義されているクライアントをリストし、クライアントが追加されていることを確認します。

```
[TestLunaSA1] lunash:>client list
registered client 1: cg-nms
registered client 2: hsm_client_name
Command Result : 0 (Success)
```

   c. クライアントをパーティションに割り当てます。

```
[TestLunaSA1] lunash:>client assignPartition -c hsm_client_name -p partition_name
'client assignPartition' successful.
Command Result : 0 (Success)
```

   d. HSM からログアウトします。

10. HSM クライアントを実行しているサーバ上で、HSM クライアントのインストールを確認します。

```
vtl verify
The following Luna SA Slots/Partitions were found:
Slot    Serial #    Label
====    ========    =====
1    151285008     TestPart1
```

11. HSM クライアントのインストールが完了したら、テスト スイートの ckdemo を実行します。

```
ckdemo
Ckdemo is the property of SafeNet Inc and is provided to our customers for
diagnostic and development purposes only.  It is not intended for use in
production installations.  Any re-distribution of this program in whole or
in part is a violation of the license agreement.

CrystokiConnect()            (modified on Oct 18 2012 at 20:57:53)

*** CHRYSTOKI DEMO - SIMULATION LAB ***
```

```
Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup.MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 1

Slots available:
    slot#1 - LunaNet Slot
    slot#2 - Luna UHD Slot
    slot#3 - Luna UHD Slot
    slot#4 - Luna UHD Slot
Select a slot: 1

SO[0] or normal user[1]?

You must enter a number between 0 and 1: 1

Status: Doing great, no errors (CKR_OK)
```

```
TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup.MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 3
Security Officer[0]
Crypto-Officer  [1]
Crypto-User     [2]: 1
Enter PIN          : 9JT5-WMYG-E5FE-TExs

Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
```

```
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup.MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 27

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000: -1

No objects found

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000: 0
ERROR: Can not find object with handle 0

Status: C_GetObjectSize returned error.(CKR_OBJECT_HANDLE_INVALID)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
```

```
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup.MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 0

Exiting GESC SIMULATION LAB
```

HSM HA クライアントの設定

(注)HSM サーバが 1 つのみであっても、この項の手順を実行する必要があります。さらに、HSM サーバを含むグループを作成する必要もあります。

HSM HA クライアントを設定するには、次の手順を実行します。

1. IoT FND サーバ上への HSM クライアントのインストールの説明に従って、HSM クライアントを設定し、両方の HSM サーバと接続するようにします。
2. /usr/safenet/lunaclient/bin/ ディレクトリに移動します。

```
/usr/safenet/lunaclient/bin/
```

3. このコマンドを実行して、最初の HSM サーバのパーティションのみを含むグループを作成します。それからパーティションにアクセスするために、**./vtl verify** コマンド(10.)を実行して取得した HSM サーバのシリアル番号(*serial_num*)、グループ名(*group_name*)、およびパスワード(*prtn_password*)を入力します。

   ./vtl haAdmin newGroup -serialNum *serial_num* **-label** *group_name* **-password** *prtn_password*

   次に例を示します。

```
./vtl haAdmin newGroup -serialNum 151285008 -label testGroup1 -password TestPart1

Warning:  There are 2 objects currently on the new member.
          Do you wish to propagate these objects within the HA
          group, or remove them?

          Type 'copy' to keep and propagate the existing
          objects, 'remove' to remove them before continuing,
          or 'quit' to stop adding this new group member.
          > copy

New group with label "testGroup1" created at group number 1151285008.
Group configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008
                    Needs sync:  no
```

4. 2 番目の HSM のパーティションをグループに追加します。

次に例を示します。

```
./vtl haAdmin addMember -group testGroup1 -serialNum 151268008 -password TestPart1
Member 151268008 successfully added to group testGroup1.New group
configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008, 151268008
                    Needs sync:  yes

Please use the command 'vtl haAdmin -synchronize' when
you are ready to replicate data between all members of the
HA group.(If you have additional members to add, you may
wish to wait until you have added them before synchronizing
to save time by avoiding multiple synchronizations.)
```

5. 両方のパーティションをリストできることを確認します。

```
./vtl haAdmin -listGroups

If you would like to see synchronization data for group testGroup1,
please enter the password for the group members.(Press enter to
skip the synchronization check):
> *********

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008, 151268008
                    Needs sync:  yes

          HA auto recovery:  disabled
                HA logging:  disabled
```

6. HA 自動リカバリを有効にします。

```
[root@localhost bin]# ./vtl haAdmin -autoRecovery

vtl haAdmin -autoRecovery [ -retry <count> | -interval <seconds> ] -retry <retry count>
-interval <seconds>
```

   - **retry** 値を -1 ～ 500 の間で設定します。ここで -1 は回数制限なく無限に再試行することを示し、0 は自動再試行を無効にすることを示します。
   - 自動リカバリのポーリング**間隔**を秒単位で指定します。

7. HA を有効にします。

```
./vtl haAdmin -HAOnly -enable
```

HSM のグループ名とパスワードの設定

HSM のグループ名とパスワードは、製造時にシスコにより提供されます。

ユーザが設定した HSM グループ名とパスワードを許可するには、次の手順を実行します。

1. **cgms.properties** ファイルを編集して、次のプロパティを追加します。

- hsm-keystore-name *<name>*
- hsm-keystore-password *<encrypted password>*

ヒント:HSM サーバ上に複数のパーティションを作成し、HSM クライアントを設定し、cgms.properties ファイル内にパーティション名とパーティション パスワードを指定することで、複数の IoT FND インストール システムに対して同じ HSM サーバを使用できます。

2. cgms.properties ファイルを保存します。
3. これらの変更を適用するには、IoT FND を再起動します。

```
service cgms start
```

ユーザ アクセスの管理

ここでは、IoT FND におけるユーザおよびロールの管理に関する次の内容について説明します。

- パスワード ポリシーの管理
- リモート認証の設定
- ロールの管理
- ユーザの管理

すべてのユーザ管理アクションは、[Admin] >[Access Management] メニューによりアクセスします(図 1)。

図 1　　[Admin] メニュー

パスワード ポリシーの管理

IoT FND は、IoT FND ユーザに適用できるデフォルトのパスワード ポリシー値を提供しています。

(注) これらの値を変更するには、root または管理者業務の権限を持つユーザとしてログインする必要があります。

注意:場合によっては、パスワード ポリシーの変更により、すべてのユーザ セッションがただちに終了し、すべてのパスワードをリセットします。

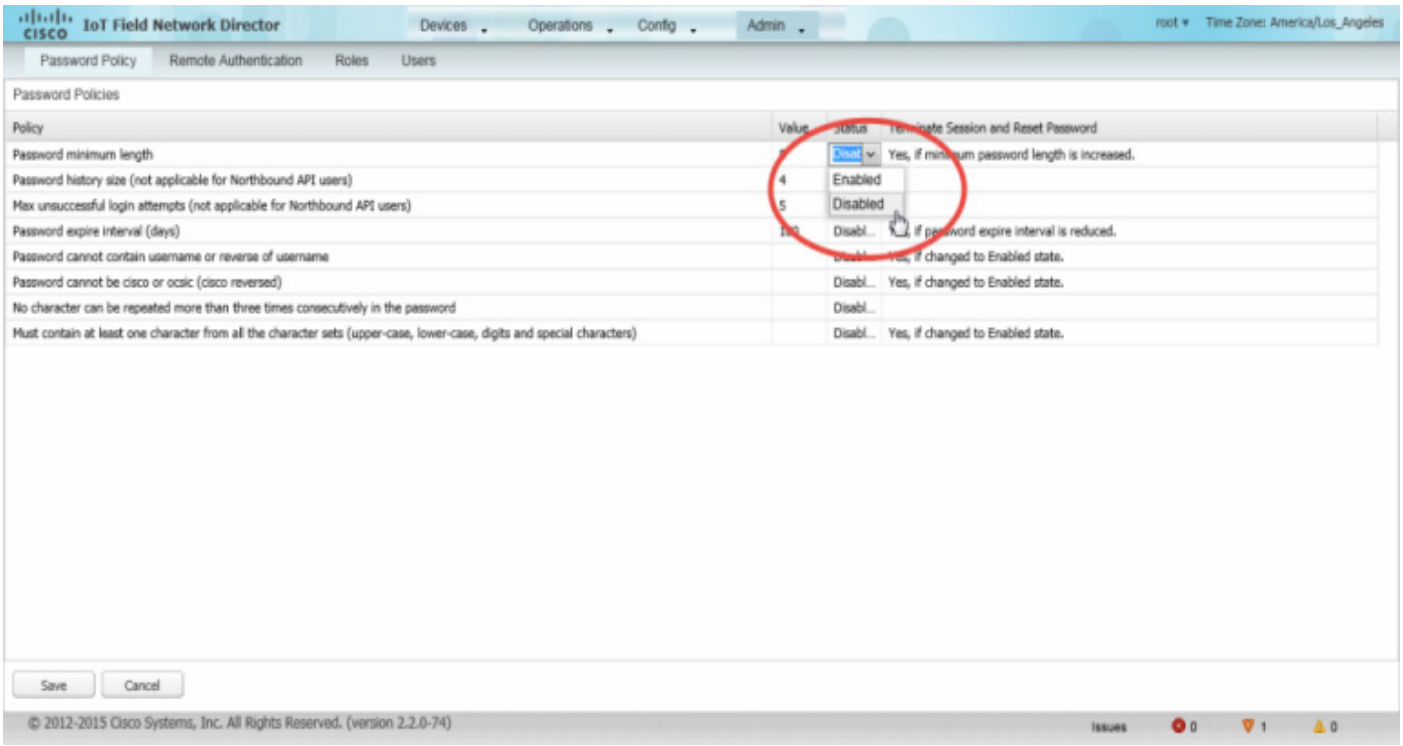
(注)「パスワード履歴サイズ」と「ログイン試行失敗の最大数」ポリシーは、IoT FND North Bound API のユーザには適用されません。

これらの変更は、以下の場合にすべてのユーザ セッションを*無効にし*、パスワードを期限切れにします（root ユーザを含む）。

- パスワードの最小長を増やしたとき
- パスワード期限間隔を減らしたとき
- [Password cannot contain username or reverse of username] を有効化したとき
- [Password cannot be cisco or ocsic (cisco reversed)] を有効化したとき
- [No character can be repeated more than three times consecutively in the password] を有効化したとき
- [Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)] を有効化したとき

パスワード ポリシーを変更するには、次の手順に従います。

1. [Admin] > [Access Management] > [Password Policy] を選択します。



2. ポリシーを有効化または無効化するには、[Status] ドロップダウン メニューから、該当するオプション（[Enabled] または [Disabled]）を選択します。
3. ポリシーの値を必要に応じて変更するには、[Value] フィールドに新しい値を入力します。

   （注）IoT FND推奨されるパスワードの最小長は 32 文字です。
4. [Save] をクリックして新しいポリシーの適用を開始します。

   （注）IoT FND で設定したパスワード ポリシーは、ローカル ユーザにのみ適用され、リモートの Active Directory（AD）ユーザには適用されません。AD ユーザに対するパスワード ポリシーは、AD 管理者によって決定、適用されます。

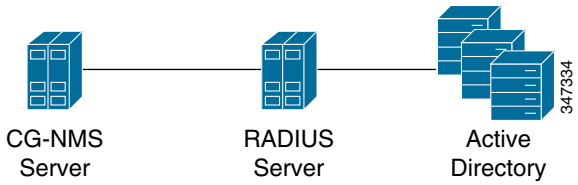
リモート認証の設定

IoT FND のリモート認証を設定するには、Active Directory（AD）および IoT FND の設定手順を実行する必要があります。

リモート認証のサポート

リモート認証では、IoT FND を既存の AD とネットワーク ポリシー サーバ（NPS）インフラストラクチャに統合するのが簡単です。これにより、管理者は AD のユーザの IoT FND へのアクセスを設定することができます。

リモート認証を IoT FND に設定すると、認証と認証責任を AD と NPS に引き渡します。AD はユーザ認証を行い、ユーザ クレデンシャルの有効性を確認します。RADIUS サーバはユーザ認証を行い、ユーザがユーザ ロールを定義するグループに属しているかどうかを確認します。属している場合、サーバはロール名を IoT FND に返します。



以下は、AD と NPS によるユーザ認証と認可のフローです。

1. ユーザが認証情報を入力します。
   - ユーザが NMS サーバでローカルに作成された場合、認証はローカルで実行されます。
   - IoT FND が、ユーザはリモート ユーザであると判断すると、認証は設定済みの RADIUS サーバで実行されます。
   - リモート認証が設定されていない場合、認証は失敗し、ユーザはアクセスを拒否されます。
2. リモート ユーザに関しては、認証が成功すると、割り当てられたユーザ ロールが、RADIUS サーバから NMS サーバに返されます。
3. 返されたロールが有効だった場合、ユーザはアクセスを許可されます。

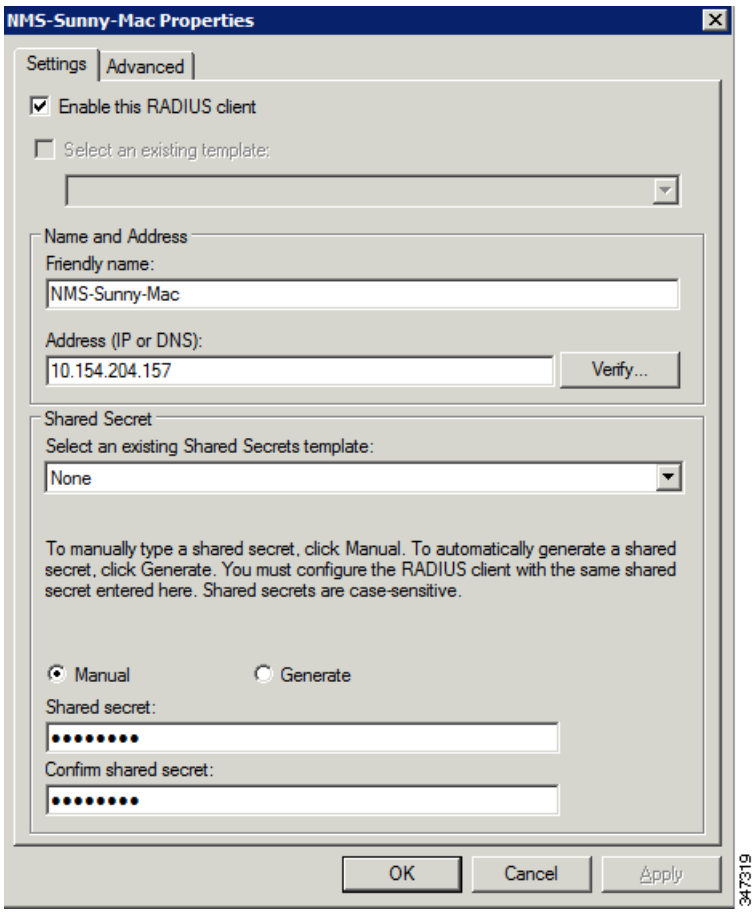
   (注) リモート認証を有効にすると、ユーザ管理は AD で実行されます。IoT FND から削除された AD ユーザがログインした場合、そのプロファイルは IoT FND に再度追加されます。IoT FND へのアクセスを防止するため、その AD ユーザ プロファイルは、最初に AD から削除する必要があります。

AD でのリモート認証の設定

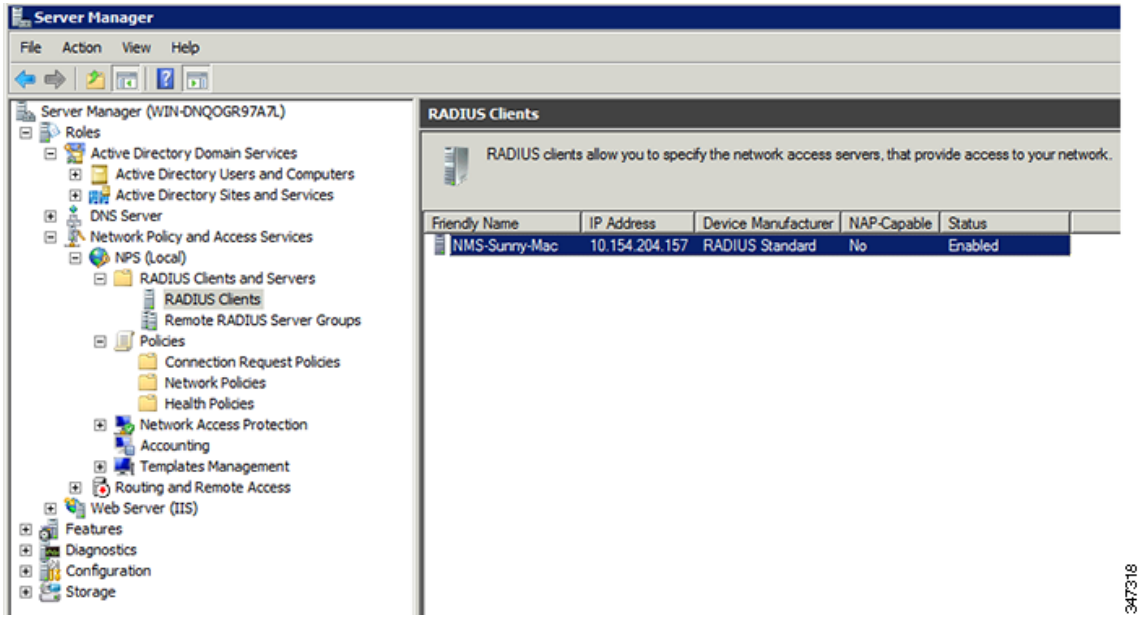
IoT FND がリモートでユーザ認証できるように AD を設定する方法:

1. NPS にログインします。
2. IoT FND を RADIUS サーバの RADIUS クライアントとして追加します。

   IoT FND サーバのフレンドリ名と IP アドレスまたは DNS 名を提供し、IoT FND が RADIUS サーバへの接続に使用する共有秘密を設定します。

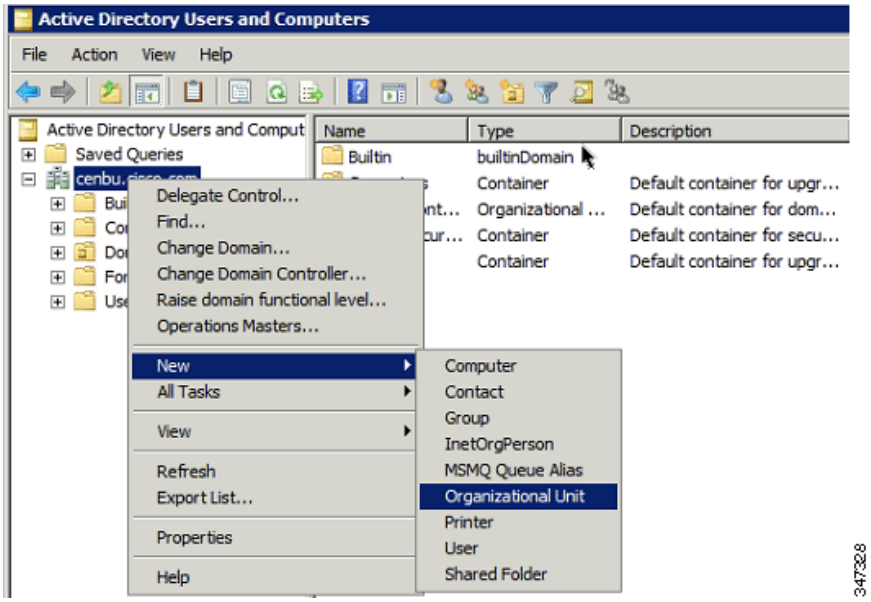


   RADIUS クライアントのエントリが、RADIUS クライアントとサーバの下に表示されます。



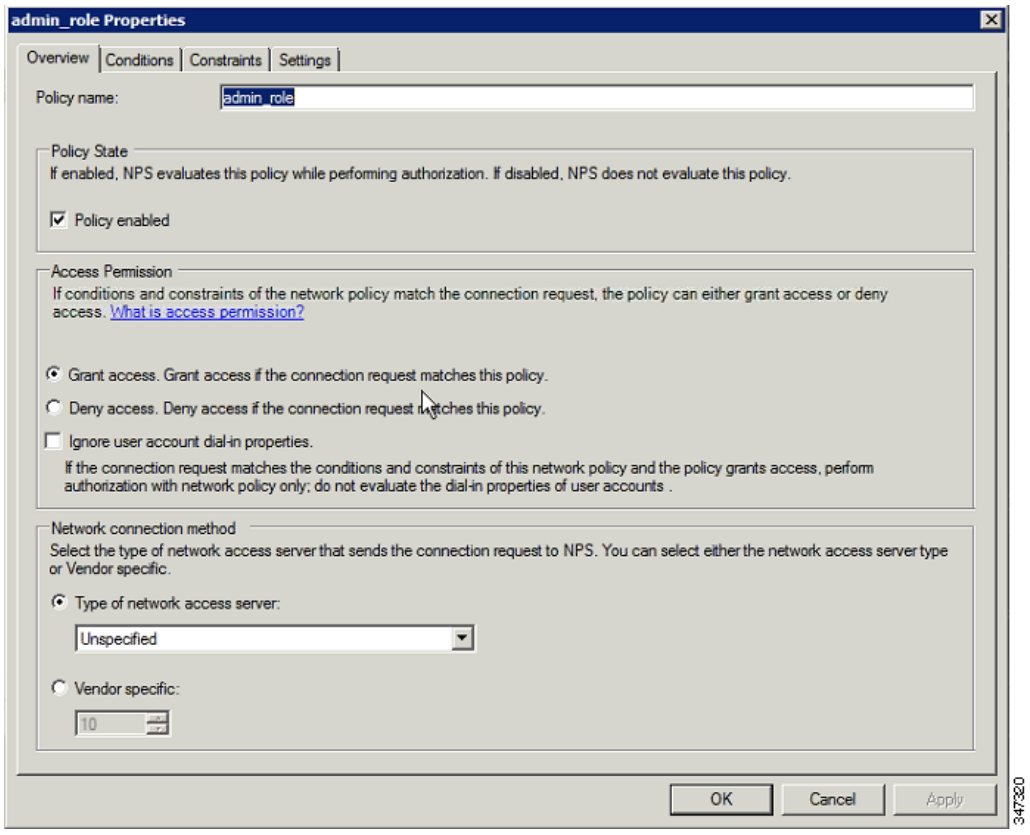
3. AD にログインし、組織単位を作成します。

   シスコはすべてのセキュリティ グループ（IoT FND ロール）をこの組織単位内に作成することを推奨します。



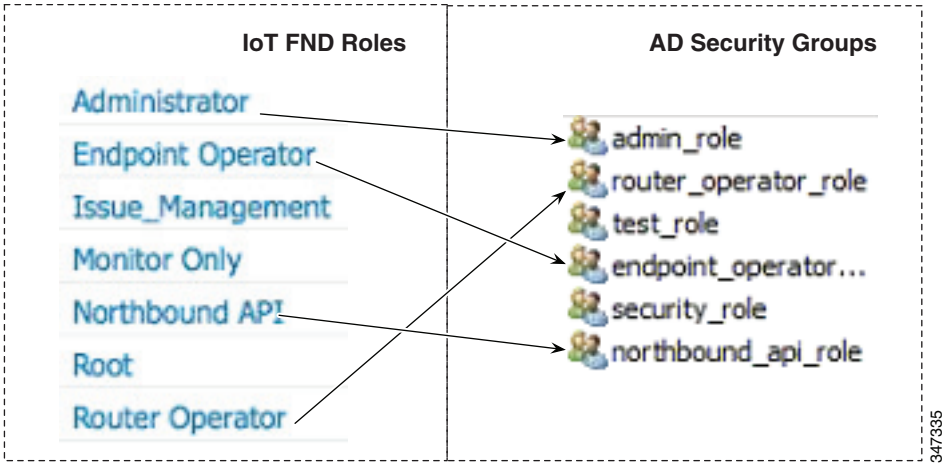
4. IoT FND のロールに対応するセキュリティ グループを組織単位に追加します。

   次の例は、NMS_ROLES 組織単位に定義されたセキュリティ グループを示します。



ヒント:セキュリティ グループを作成するときは、それらが IoT FND ロールに 1 対 1 でマッピングされている（つまり IoT FND に定義された各ロールが、1 つの AD セキュリティ グループにのみマッピングされている）ことを確認します。セキュリティ グループの名前は IoT FND のロール名と一致する必要はありませんが、組織的な目的から、シスコは セキュリティ グループの名前を IoT FND ロールに関連付ける名前を使用することを推奨します。

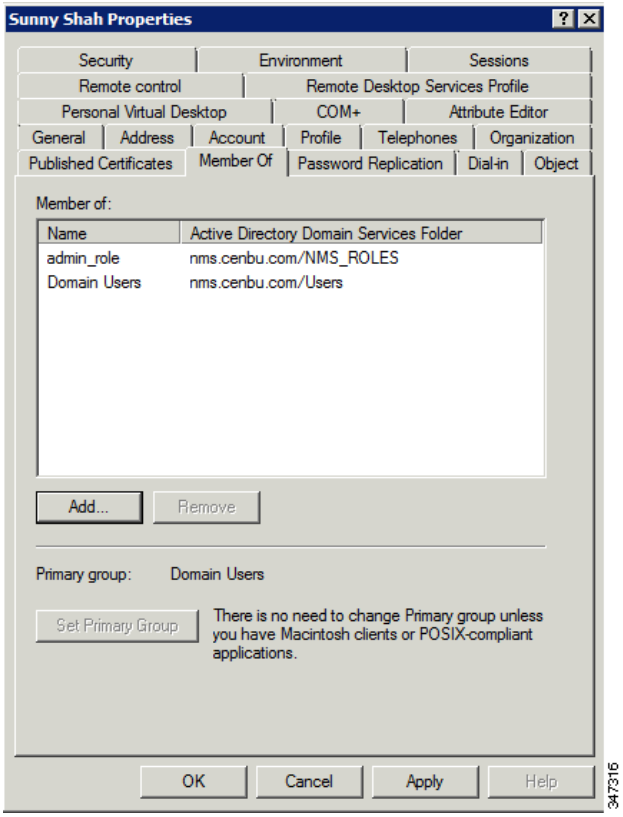
(注)AD に IoT FND root ロールを作成または割り当てることはできません。



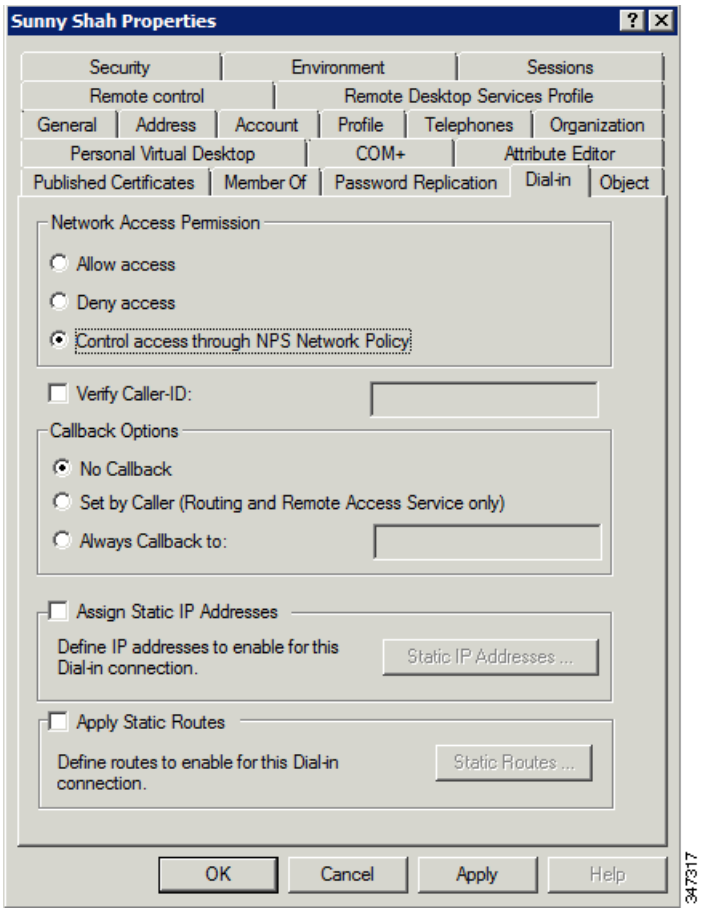
5. AD ユーザをロールへのセキュリティ グループ マッピングに追加することで、ユーザをそのロールに割り当てます。

ユーザは 1 つのセキュリティ グループにのみ属することができるため、ユーザがログイン後に割り当てられる IoT FND のロールは、割り当てられた AD セキュリティ グループによって決まります。

ヒント:AD では、ユーザは複数の IoT FND ロールに割り当てられたり、複数のセキュリティ グループに属したりすることはできません。複数のロールからユーザ グループにアクセス許可を割り当てるには、必要なアクセス許可のある新しい IoT FND ロールを作成し、対応する AD セキュリティ グループを作成します。この新しいグループのユーザはその後、このロールによって許可されているタスクを実行できます。



6. ダイヤルイン ネットワーク アクセス権を設定して、NPS のネットワーク ポリシーを使用します。

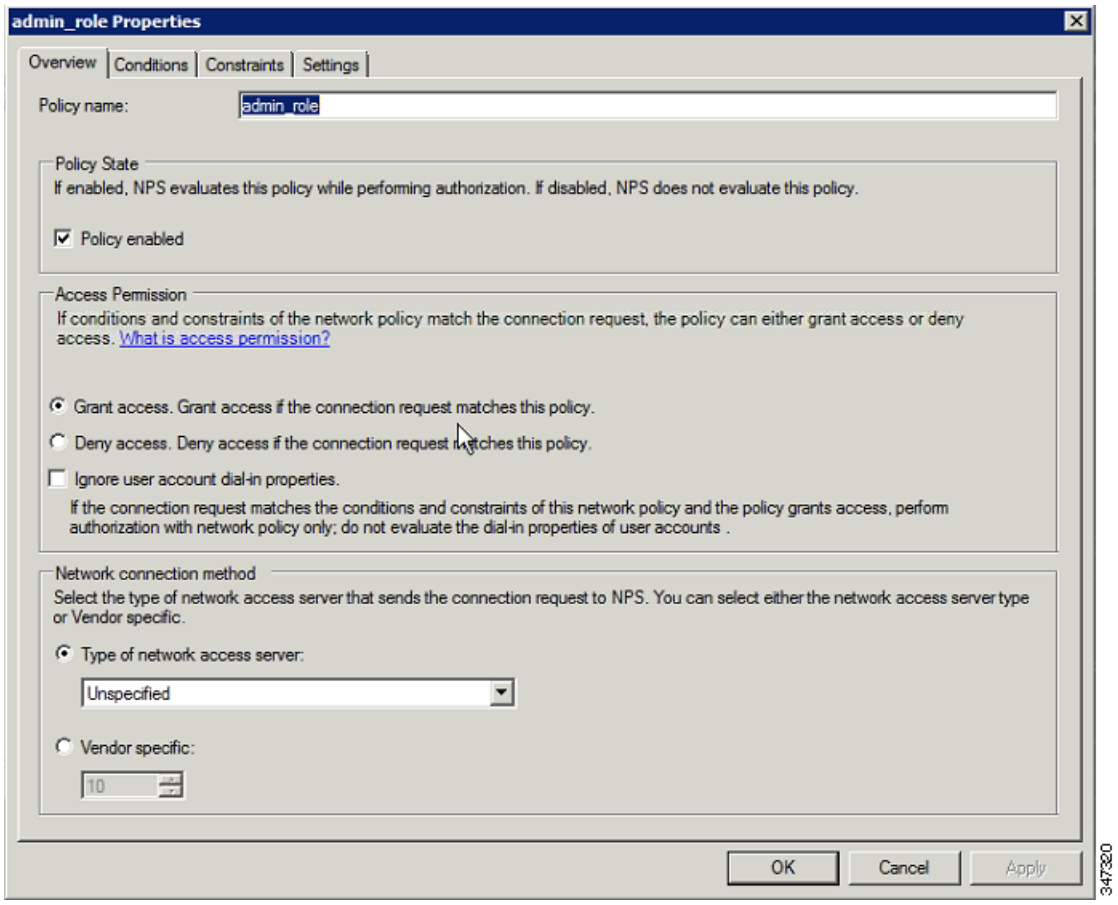


RADIUS サーバ セキュリティ ポリシーの設定

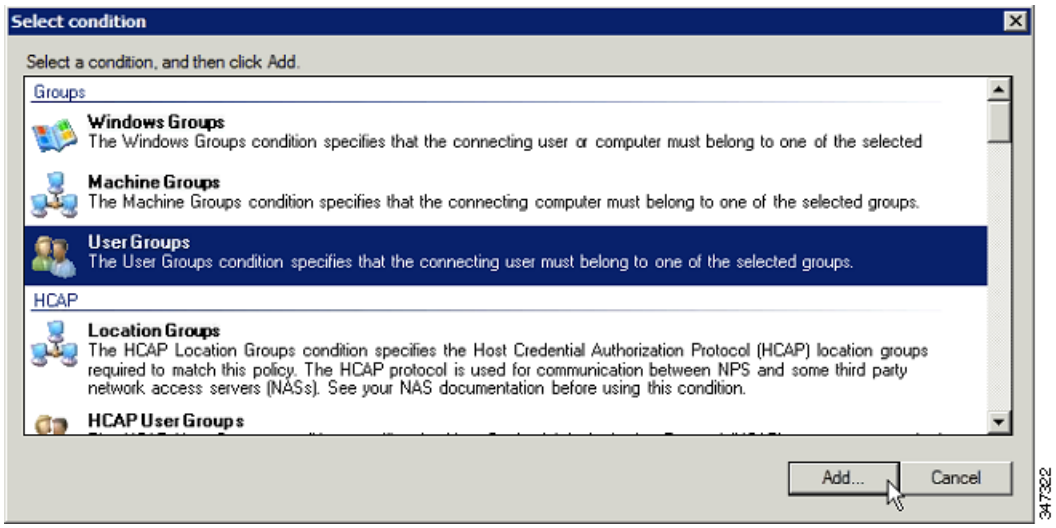
IoT FND にアクセスするユーザを認証するには、RADIUS サーバのセキュリティ ポリシーを設定します。

RADIUS サーバにセキュリティ ポリシーを設定するには、次の手順に従います。

1. ユーザが AD に作成した各セキュリティ グループのネットワーク ポリシーを作成します。
2. ポリシーを次のように設定します。
   a. [Overview] ペインでポリシー名を定義して有効にし、アクセス権限を付与します。

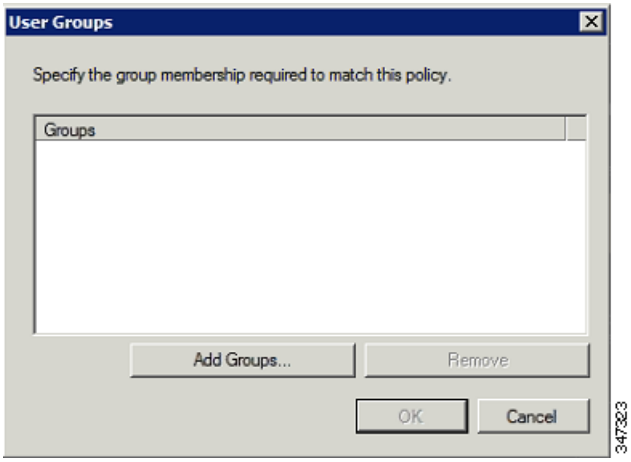


b. [Conditions] タブをクリックして、[User Groups] を選択し、[Add] をクリックします。



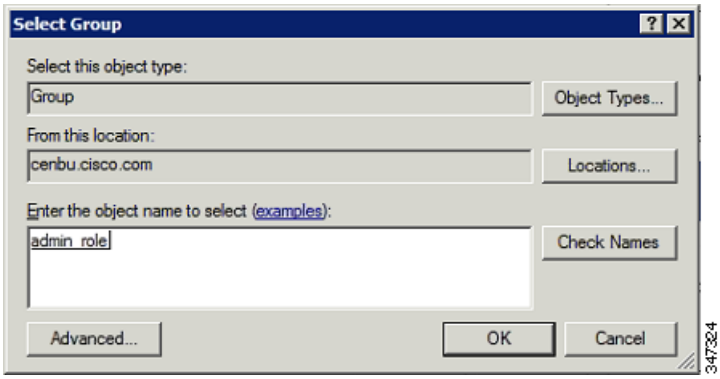
[User Groups] の条件は、接続するユーザが選択したグループに属する必要があることを指定します。このポリシーが条件を満たすには、認証されているユーザがこのポリシーで設定されるユーザ グループに属している必要があります。

c. [User Groups] ウィンドウで、[Add Groups] をクリックします。



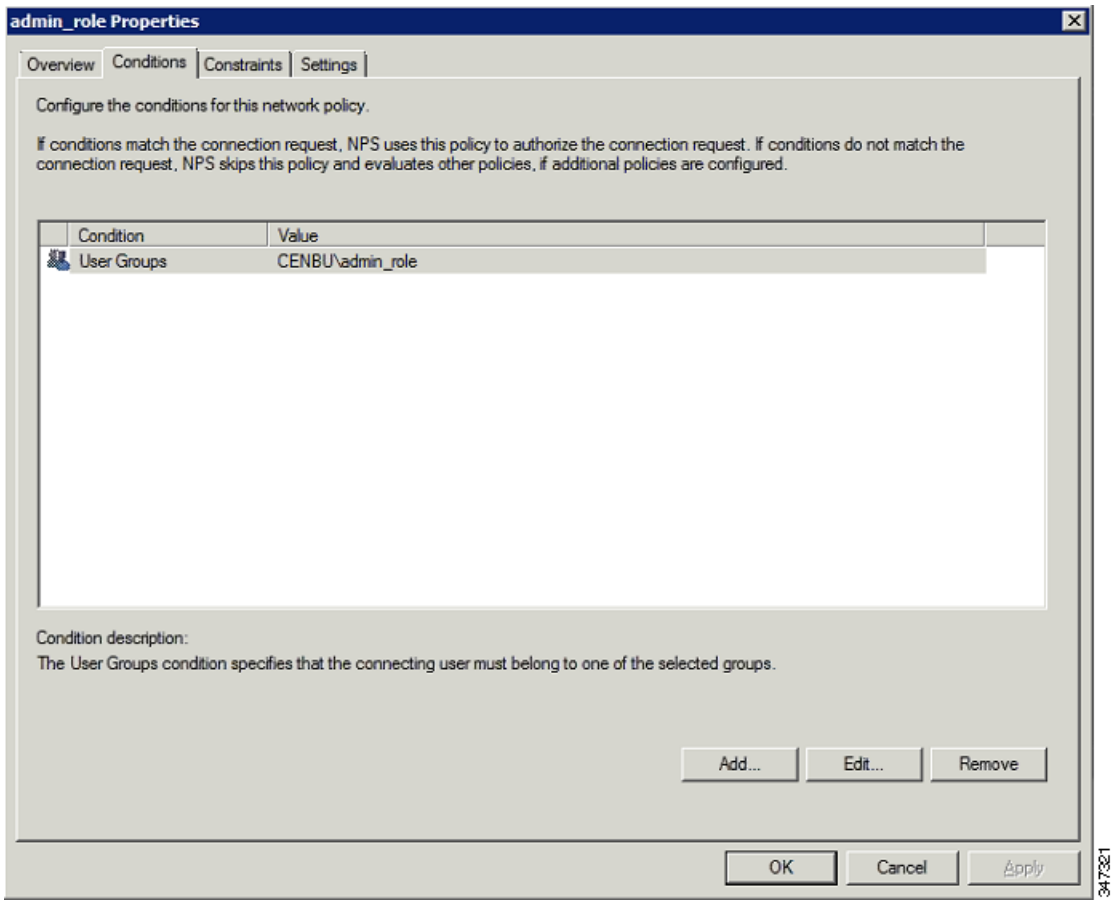
d. [Select Group] ウィンドウで、グループの名前を入力します。

e. [OK] をクリックして [Select Group] ダイアログボックスを閉じ、次に [OK] をクリックして [User] ダイアログボックスを閉じます。

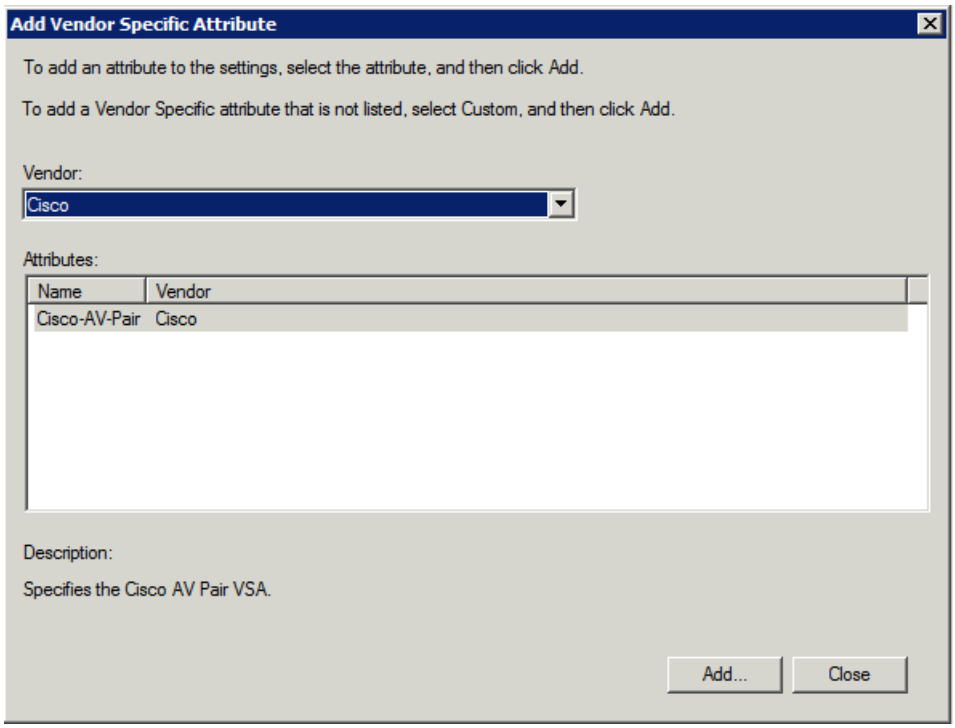


f. [Cancel] をクリックして、[Select condition] ウィンドウを閉じます。

[Conditions] ペインに条件が表示されます。



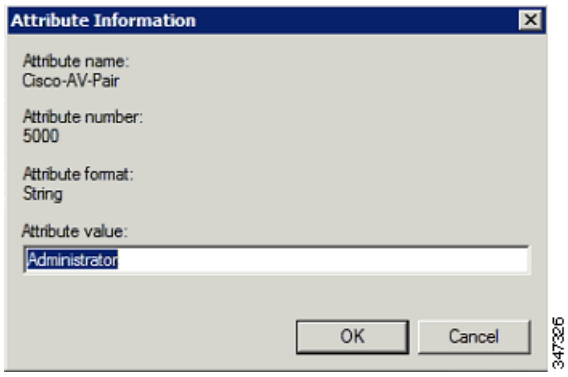
g. [Settings] タブをクリックし、[Add] をクリックして [Attribute Information] ウィンドウを表示します。



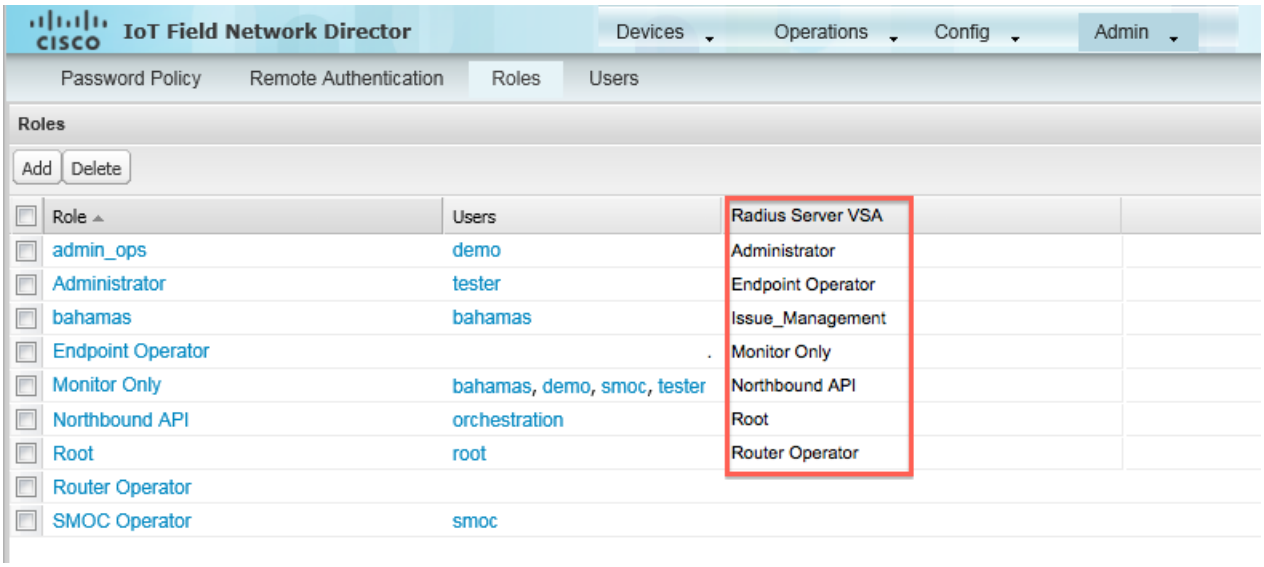
h. [Add] をクリックして、ユーザ クレデンシャルとセキュリティ グループのメンバーシップが確認された後に IoT FND（RADIUS クライアント）に送信される [Vendor Specific Attribute]（VSA）を定義します。

設定する VSA は次のとおりです。

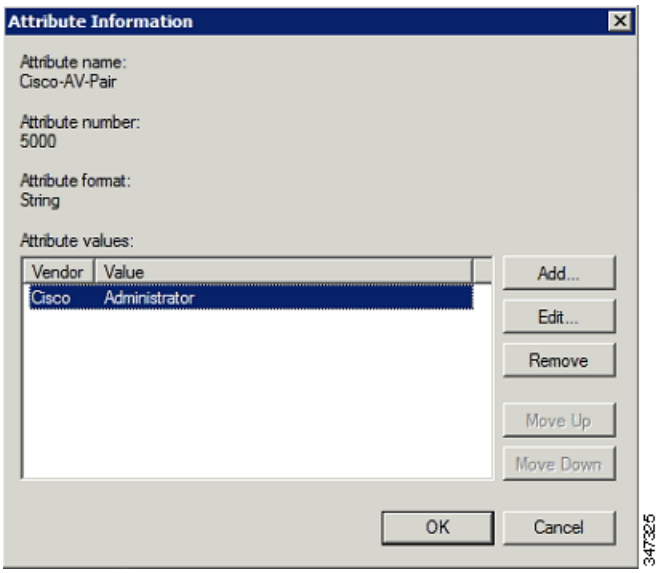
- Attribute Name：Cisco-AV-Pair
- Attribute number：5000
- Attribute format：String
- Attribute value：IoT FNDに送る属性値を入力します。



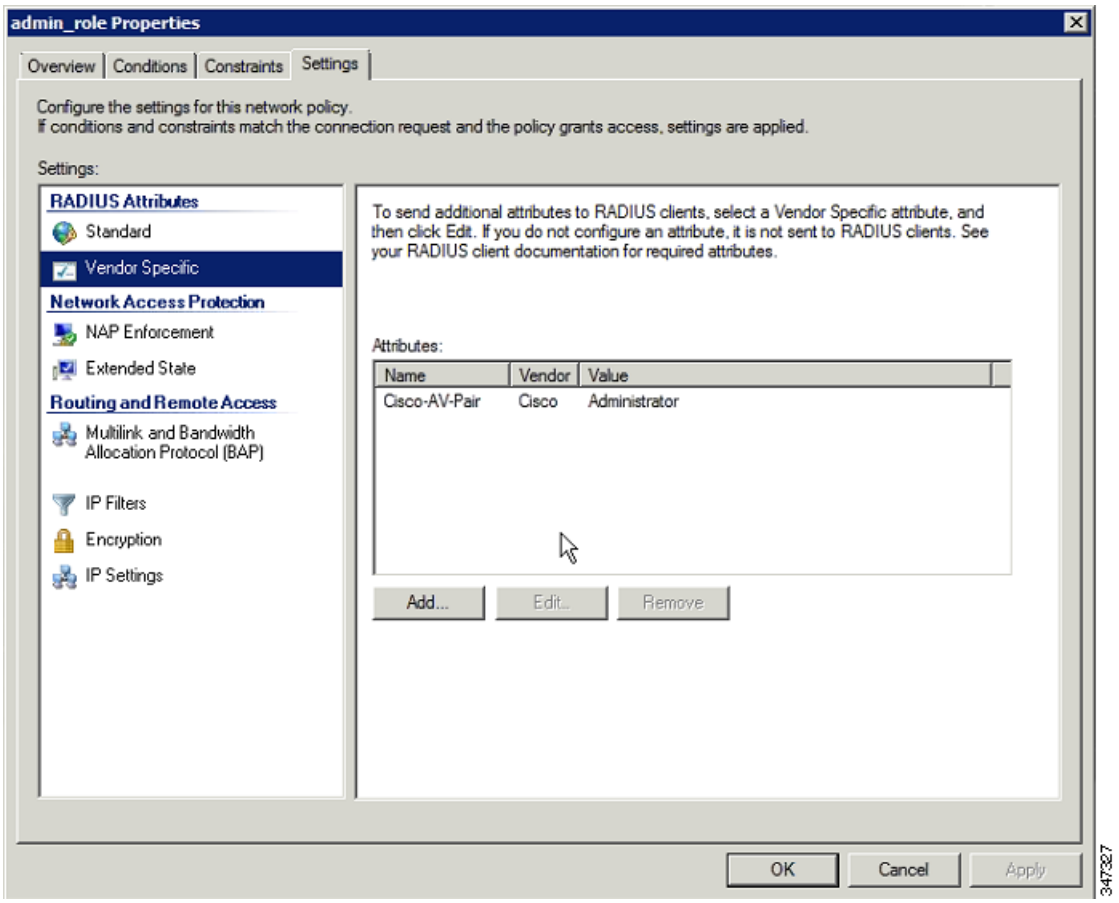
(注) [Attribute value] フィールドに入力されるストリングは、IoT FND の [Roles] ページの [Radius Server VSA] 列に表示される正確な文字列である必要があります（[Admin] > [Access Management] > [Roles]）。



i. [OK] をクリックします。



VSA の属性が [Settings] ペインに表示されます。



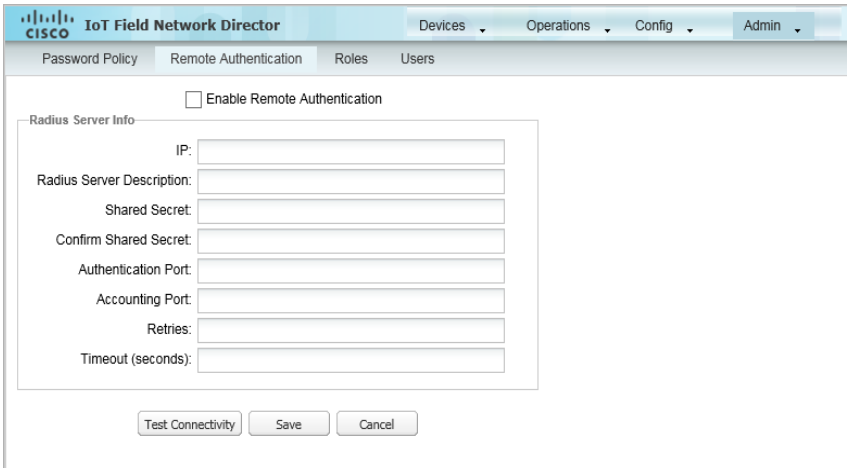
j. [OK] をクリックします。

IoT FND でのリモート認証の設定

リモート ユーザ認証を有効にして、[Remote Authentication] ページで RADIUS サーバを設定します([Admin] > [Access Management] > [Remote Authentication])。

リモート認証の設定方法:

1. [Admin] > [Access Management] > [Remote Authentication] の順に選択します。



2. [Enable Remote Authentication] チェックボックスをオンにします。
3. RADIUS サーバに関する以下の情報を入力します。

フィールド	説明
IP	RADIUS サーバの IP アドレス。
名前	RADIUS サーバのわかりやすい名前。
Shared Secret	ユーザが RADIUS サーバで設定した共有秘密。
Confirm Shared Secret	
Authentication Port	IoT FND が要求を送信するときに使用する RADIUS サーバ ポート。デフォルト ポートは 1812 です。
Accounting Port	RADIUS サーバ アカウンティング ポート。デフォルト ポートは 1813 です。
Retries	IoT FND がタイムアウトし、RADIUS サーバからの応答が受信されずリモート認証が失敗するまでに、RADIUS サーバにリクエストを送信する回数。
Timeout	IoT FND がタイムアウトし、RADIUS サーバからの応答が受信されずリモート認証が失敗するまでの秒数。

4. IoT FND の RADIUS サーバへの到達を確認するには [Test Configuration] をクリックします。
   a. AD のユーザ名とパスワードを入力します。
   b. [Submit] をクリックします。`

   設定テストの結果が表示されます。
   c. [OK] をクリックします。
5. 完了したら、[Save] をクリックします。

リモート ユーザ アカウントの有効化と無効化

IoT FND では、AD ユーザ アカウントをリモートで有効または無効にすることはできません。リモート AD ユーザ アカウントを有効または無効にするには、AD サーバを使用します。

リモート ユーザ アカウントの削除

IoT FND で、リモート ユーザ アカウントを削除できます。ただし、これは IoT FND の [Users] ページ([Admin] > [Access Management] > [Users])からユーザを削除するのみで、AD からユーザ アカウントを削除することはありません。削除されたユーザが IoT FND にログインし、AD 認証が成功すると、ユーザのエントリが、IoT FND の [Users] ページに追加されます。

リモート ユーザ アカウントを使用したIoT FND へのログイン

リモート AD ユーザ アカウントを使用した IoT FND へのログインはユーザーに対しトランスペアレントです。バックグラウンドでは、IoT FND はアカウントがローカルであるかどうかをチェックし、リモート ユーザには [Remote Authentication] ページで設定した RADIUS サーバに認証要求を送信します([Admin] > [Access Management] > [Remote Authentication])。認証に成功したら、IoT FND はユーザのエントリを [Users] ページで追加します([Admin] > [Access Management] > [Users])。

[Users] ページのローカル ユーザのエントリとは異なり、リモート ユーザのエントリにファイルされたユーザ名は、リンクではありません。ユーザに関する詳細情報を得るためにリモート ユーザの名前をクリックすることはできません。

(注)IoT FND でリモート ユーザを管理することはできません。リモート ユーザがパスワードを更新するには、組織の AD パスワード更新ツールを使用する必要があります。リモート ユーザは IoT FND を使用して自分のパスワードを更新できません。

ロールの管理

ロールを使用して、ユーザが務めるロールに基づいたアクセス許可を割り当てます。ロールは、IoT FND のユーザが実行できるタスクのタイプを定義します。ここでは、次の内容について説明します。

- ロールの追加
- ロールの削除
- ロールの編集
- ロールの表示

IoT FND を使用すると、すべてのユーザにロールを割り当てることができます。ユーザが実行できる操作は、そのロール対して有効なアクセス許可に基づいています。ここでは、次の内容について説明します。

- 基本ユーザ権限
- システム定義ユーザー ロール
- カスタム ユーザ ロール

基本ユーザ権限

表 1 で、基本的な IoT FND のアクセス許可について説明します。

表 1　　IoT FND のユーザ権限

権限	説明
Add/Modify/Delete Devices	ユーザに FAR およびエンドポイント デバイスのインポート、削除、変更を許可します。
Administrative Operations	ユーザにユーザ管理、ロール管理、サーバ構成設定などのシステム管理操作の実行を許可します。
Endpoint Configuration	ユーザに設定テンプレートの編集と、ME への設定のプッシュを許可します。
Endpoint Firmware Update	ユーザにファームウェア イメージの追加と削除、ME ファームウェア アップデート操作の実行を許可します。
Endpoint Group Management	ユーザに ME 設定とファームウェア グループからのデバイスの割り当て、削除、変更を許可します。
Endpoint Reboot	ユーザに ME デバイスの再起動を許可します。
GOS Application Management	ユーザにゲスト OS アプリケーションの追加と削除を許可します。
Issue Management	ユーザに問題をクローズする許可を与えます。
Label Management	ユーザにラベルの追加、変更、削除を許可します。
Manage Device Credentials	ユーザに WiFi 事前共有キー、管理者ユーザ パスワード、マスター キーなどの FAR クレデンシャルの表示を許可します。
Manage Head-End Devices Credentials	ユーザに ASR 管理者 NETCONF パスワード表示を許可します。
NBAPI Audit Trail	ユーザに IoT FND の NB API を使用した監査証跡のクエリと削除を許可します。
NBAPI Device Management	ユーザに IoT FND の NB API を使用した FAR およびエンドポイント デバイスの追加、削除、エクスポート、変更を許可します。
NBAPI Endpoint Operations	ユーザに IoT FND の NB API を使用したエンドポイント操作の管理を許可します。
NBAPI Event Subscribe	ユーザに IoT FND の NB API を使用したイベント（停止イベントなど）の検索、登録、登録解除を許可します。
NBAPI Reprovision	ユーザに IoT FND の NB API を使用したデバイスの再プロビジョニングを許可します。

表 1　IoT FND のユーザ権限（続き）

権限	説明
NBAPI Rules	ユーザに IoT FND の NB API を使用したルールの検索、作成、削除、有効化、無効化を許可します。
NBAPI Search	ユーザに IoT FND の NB API を使用したデバイスの検索、デバイスの詳細取得、グループ情報取得、メトリック履歴取得を許可します。
ルータ設定	ユーザに FAR 設定テンプレートの編集、FAR への設定のプッシュを許可します。
Router Firmware Update	ユーザにファームウェア イメージの追加と削除、FAR のファームウェア アップデート操作の実行を許可します。
Router Group Management	ユーザに FAR 設定とファームウェア グループへのデバイスの割り当て、削除、変更を許可します。
Router Reboot	ユーザに FAR の再起動を許可します。
Rules Management	ユーザにルールの追加、編集、有効化、無効化を許可します。
セキュリティ ポリシー	ユーザに メッシュ デバイスのブロック、メッシュ キーの更新などを許可します。
Tunnel Provisioning Management	ユーザにトンネル グループの管理、トンネル関連のテンプレートの編集と適用、出荷時再プロビジョニングの実行を許可します。
Work Order Management	ユーザに IoT-DM のワーク オーダー管理を許可します。

システム定義ユーザー ロール

(注) システム定義された root ロールは、ユーザに割り当てることはできません。

表 2で、システム定義ロールを説明します。このロールは変更できません。

表 2　システム定義ユーザー ロール

ロール	説明
デバイスの追加	このロールでは、IoT FND からのデバイスの追加、変更、削除ができます。
Administrator	このロールは、以下の基本的なアクセス許可を兼ね備えています。 ■ Administrative Operations ■ Label Management ■ Rules Management
Endpoint Operator	このロールは、以下の基本的なアクセス許可を兼ね備えています。 ■ Label Management ■ Endpoint Configuration ■ Endpoint Firmware Update ■ Endpoint Group Management ■ Endpoint Reboot
Monitor Only	このロールはユーザに IoT FND への読み取り専用アクセスを提供します。このロールはデフォルトですべてのユーザに定義されます。

表 2　　システム定義ユーザー ロール(続き)

ロール	説明
North Bound API	このロールは、以下の基本的なアクセス許可を兼ね備えています。 ■ NB API Audit Trail ■ NB API Device Management ■ NB API Endpoint Operations ■ NB API Event Subscribe ■ NB API Orchestration Service ■ NB API Rules ■ NB API Search
Router Operator	このロールは、以下の基本的なアクセス許可を兼ね備えています。 ■ Label Management ■ ルータ設定 ■ Router Firmware Update ■ Router Group Management ■ Router Reboot
Router Operator with Manage Device Creds	このロールは、ルータ オペレータの権限を以下と統合します。 ■ Device credential management
セキュリティ ポリシー	このロールでは、IoT FND を介してセキュリティ ポリシーを管理できます。
Tunnel Provisioning Management	このロールはトンネルをプロビジョニングすることができます。

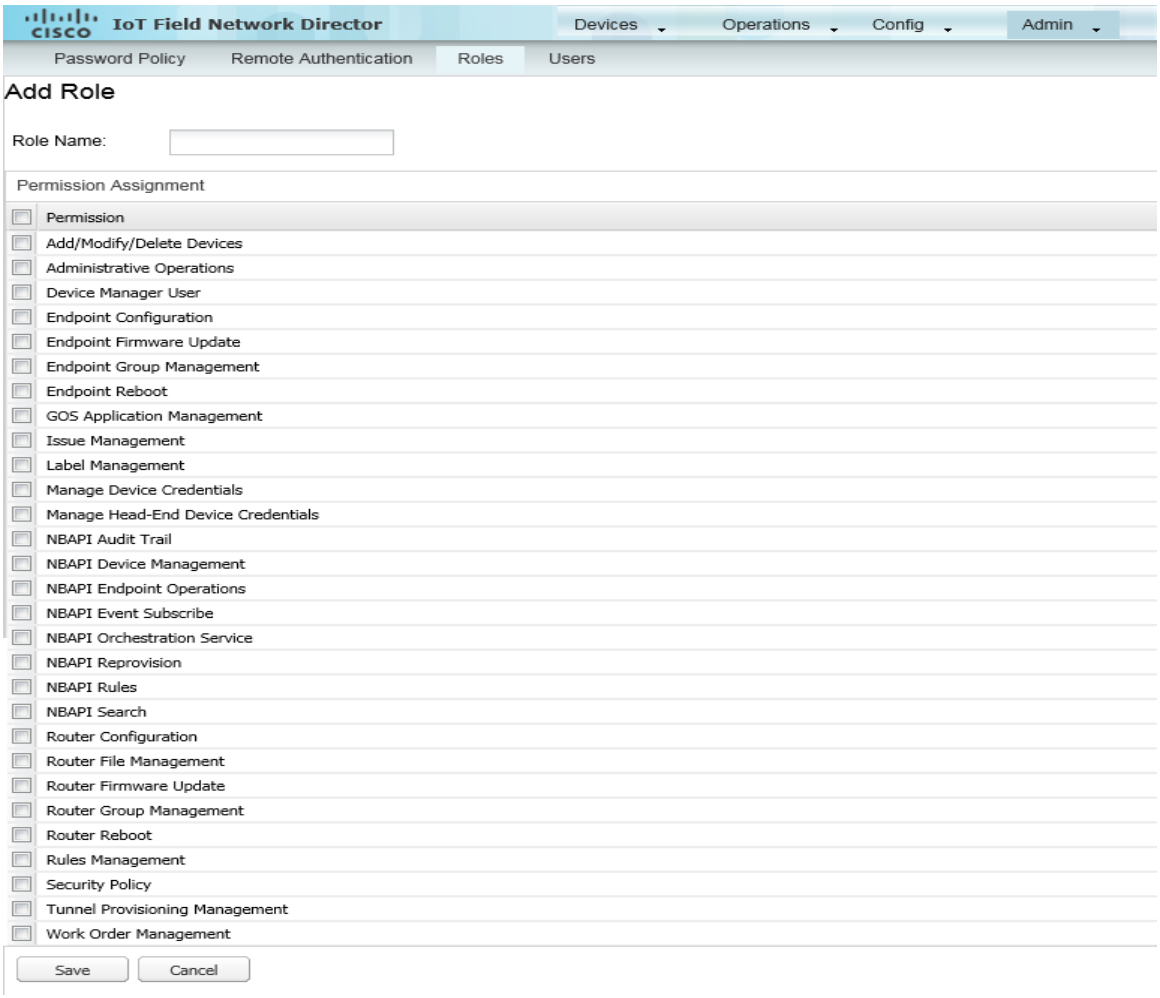
カスタム ユーザ ロール

IoT FND では、カスタム ロールを定義できます。ユーザが作成する各ロールに、1 つ以上の基本ユーザ権限を割り当てることができます(表 1 参照)。これらの権限はこのロールのユーザが実行できるアクションのタイプを指定します。

ロールの追加

IoT FND ユーザ ロールを追加するには、次の手順を実行します。

1. [Admin] > [Access Management] > [Roles] を選択します。
2. [Add] をクリックします。



3. ロールの名前を入力します。
4. 該当するチェックボックスをオンにして、権限を割り当てます。
5. [Save(保存)] をクリックします。
6. ロールの追加を続行するには [Yes] をクリックし、続行しない場合は [No] をクリックして [Roles] ページに戻ります。

ロールの削除

(注)使用中のカスタム ロールを削除することはできません。

IoT FND ユーザ ロールを削除するには、次の手順を実行します。

1. [Admin] > [Access Management] > [Roles] を選択します。
2. 削除するロールのチェックボックスをオンにします。
3. [Delete] をクリックします。
4. [Yes] をクリックします。
5. [OK] をクリックします。

ロールの編集

(注) システム定義されたロールは編集できませんが、カスタム ロールは編集できます。

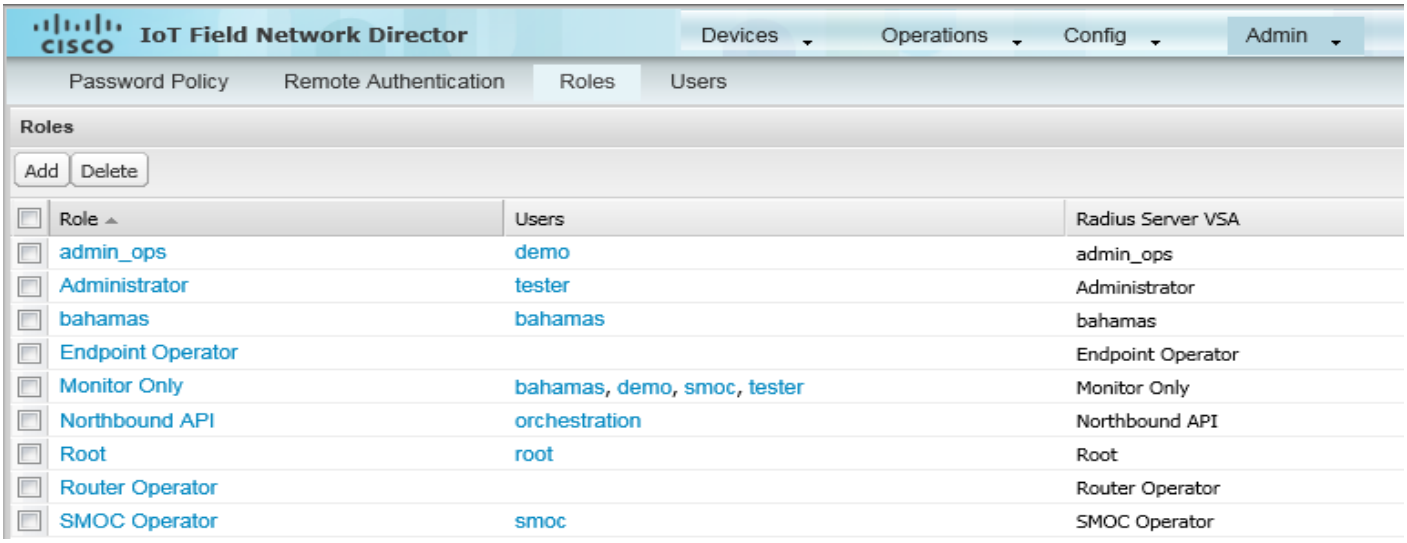
IoT FND のカスタム ロールを編集するには、次の作業を行います。

1. [Admin] > [Access Management] > [Roles] を選択します。
2. 編集するロールをクリックします。
3. 該当するチェックボックスをオンまたはオフにして、権限の割当てを変更します。
4. [Save(保存)] をクリックします。

ロールの表示

IoT FND ユーザ ロールを表示するには、次の手順を実行します。

1. [Admin] > [Access Management] > [Roles] を選択します。



   各ロールで、IoT FND はこのロールに割り当てられたユーザを表示します。

2. ロールの権限割り当てを表示するには、ロール リンクをクリックします。

ユーザの管理

ここでは、ユーザ管理に関する次の内容について説明します。

- パスワードのリセット
- ユーザの表示
- ユーザの追加
- ユーザの削除
- ユーザの有効化
- ユーザの無効化
- ユーザの編集

パスワードのリセット

IoT FND が実行される Linux サーバの root ユーザは、パスワードをリセットし、パスワード ユーティリティを使用して他の IoT FND ユーザのパスワードをリセットできます。

パスワードをリセットするには、次のコマンドを入力します。

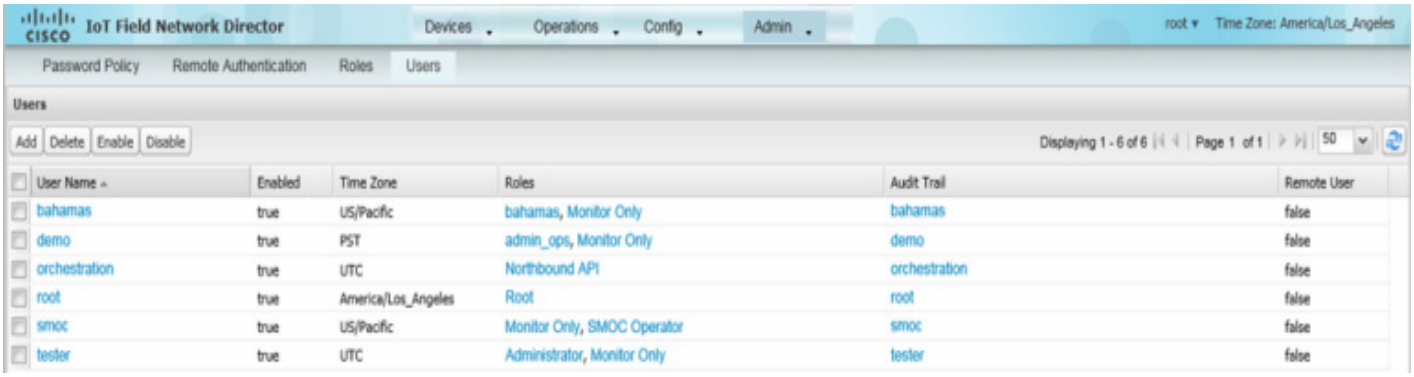
```
[root@yourname-lnx1 bin}#./password_admin.sh root
```

IoT FND はそれ自体のユーザ アカウント データベースを管理しており、そのため、すべての新しいローカル ユーザを IoT FND のユーザ インターフェイスから追加する必要があります（[Admin] > [Access Management] > [Users] ページ）。リモート ユーザはデータベースに自動的に追加されます。また、このページでユーザを有効化、無効化、編集、削除できます。

無効化されたアカウントのユーザは、管理者がこのアカウントを有効にするまでログインできません。ユーザ アカウントが有効になった後、ユーザはパスワードをリセットする必要があります。使用できるデータベース ストレージ以外に、システムで定義できるユーザの数に制限はありません。

ユーザの表示

IoT FND のユーザを表示するには、[Users] ページを開きます（[Admin] > [Access Management] > [Users]）。



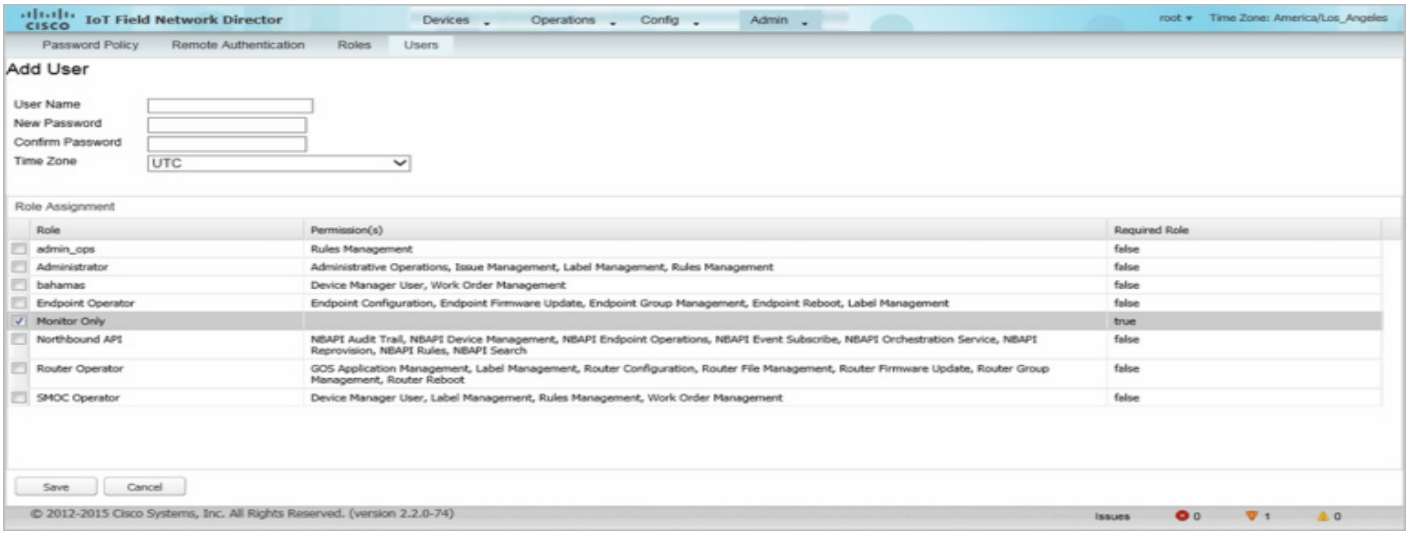
IoT FND により、ユーザに関する以下の情報が表示されます。

フィールド	説明
ユーザ名	ユーザ名を指定します。
イネーブル	ユーザ アカウントが有効化されているかどうかを示します。
Time Zone	ユーザのタイム ゾーンを指定します。
Roles	ユーザに割り当てるロールを指定します。
Audit Trail	ユーザの監査証跡へのリンク。
Remote User	ユーザ アカウントがローカルに保存されているかどうかを示します。値が False の場合、ユーザ アカウントは Active Directory に保存され、リモート認証ページで構成された RADIUS サーバ経由でアクセスできます（[Admin] > [Access Management] > [Remote Authentication]）。

ユーザの追加

ユーザを IoT FND に追加するには、以下の手順を実行します。

1. [Admin] > [Access Management] > [Users] の順に選択します。
2. [Add] をクリックします。



3. 以下のユーザ情報を入力します。

フィールド	説明
ユーザ名	ユーザ名を入力します。
New Password	パスワードを入力します。パスワードは、IoT FND パスワード ポリシーに従う必要があります。
Confirm Password	パスワードを再入力します。
Time Zone	タイム ゾーンをドロップダウン メニューから選択します。

4. [Role Assignment] の下の該当するチェックボックスをオンにして、このユーザに割り当てられているユーザ ロールを選択します。
5. [Save(保存)] をクリックします。

   IoT FND は、IoT FND データベースにこのユーザのレコードを作成します。
6. 新しいユーザを追加するには、[Yes] をクリックし、追加しない場合は [No] をクリックして [Users] ページに戻ります。

   (注) 新規ユーザ アカウントはデフォルトで有効になっています。つまり、ユーザは IoT FND にアクセスできます。

ユーザの削除

ユーザ アカウントを削除すると、デフォルトのマッピング ロケーション などのユーザ設定がシステムから削除されます。一時的にユーザ アカウントを非アクティブ化するには、ユーザ アカウントを無効にします。

IoT FND からユーザを削除するには、以下の手順を実行します。

1. [Admin] > [Access Management] > [Users] の順に選択します。
2. 削除するユーザ アカウントのチェックボックスをオンにします。

3. [Delete] をクリックします。
4. 確認のために [Yes] をクリックします。
5. [OK] をクリックします。

ユーザの有効化

IoT FND にアクセスするユーザのユーザ アカウント有効化する必要があります。ユーザが初めてログインすると、IoT FND によりパスワードの変更を求められます。

IoT FND のユーザ アカウントを有効化するには、以下の手順を実行します。

1. [Admin] > [Access Management] > [Users] の順に選択します。
2. 有効化するユーザ アカウントのチェックボックスをオンにします。
3. [Enable] をクリックします。
4. [Yes] をクリックします。
5. [OK] をクリックします。

ユーザの無効化

ユーザが IoT FND にアクセスするのを防ぐには、アカウントを無効化します。ユーザ アカウントを無効にしても、IoT FND データベースからレコードは削除されません。

IoT FND のユーザ アカウントを無効化するには、以下の手順を実行します。

1. [Admin] > [Access Management] > [Users] の順に選択します。
2. 無効化するユーザ アカウントのチェックボックスをオンにします。
3. [Disable] をクリックします。

   (注)ユーザ アカウントを無効にすると、IoT FND によりユーザのパスワードがリセットされます。
4. [Yes] をクリックします。
5. [OK] をクリックします。

ユーザの編集

IoT FND のユーザ設定を編集するには、以下の手順を実行します。

1. [Admin] > [Access Management] > [Users] の順に選択します。
2. ユーザ クレデンシャルを編集するには:
   a. ユーザ名のリンクをクリックします。
   b. ロールの割り当てを編集します。
   c. [Save(保存)] をクリックします。

システム設定の管理

この項では、システム設定の管理方法について説明します。ここで説明する内容は、次のとおりです。

- アクティブ セッションの管理
- 監査証跡の表示
- 証明書の管理
- データ保存の設定
- ライセンスの管理
- ログの管理
- プロビジョニングの設定
- サーバ設定値の設定
- Syslog の管理

(注) システム設定を管理するには、root としてログインするか、または管理操作権限を持つユーザとしてログインする必要があります。

システム設定は、[Admin] > [System Management menu] (図 1) から管理されます。

図 1　[Admin] メニュー

アクティブ セッションの管理

IoT FND は、アクティブなユーザ セッションを追跡し、ユーザをログアウトさせることができます。

- アクティブなセッションの表示
- Logging Users Out
- アクティブ セッション リストのフィルタリング

アクティブなセッションの表示

アクティブなユーザ セッションを表示するには、[Admin] > [System Management] >[Active Sessions] を選択します。IoT FND は、[Active Sessions] ページを示しています（図 2）。

図 2　[Active Sessions] ページ

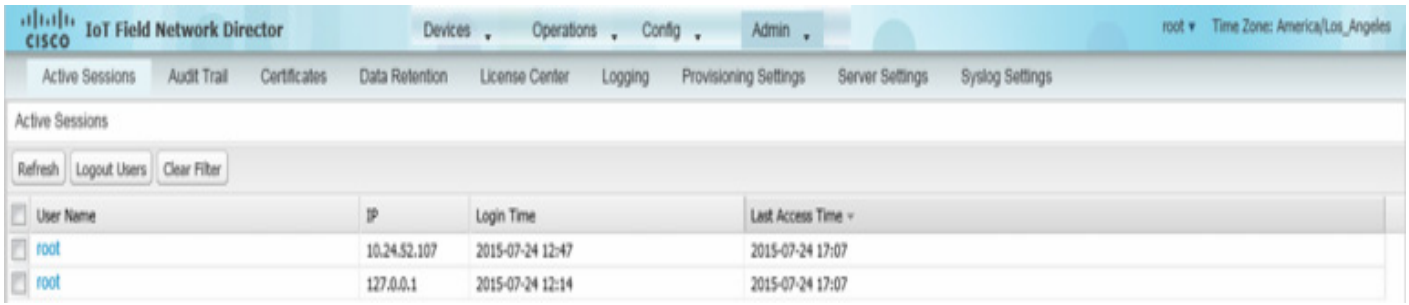


表 1 は、[Active Session] のフィールドを説明しています。

表 1　[Active Session] のフィールド

フィールド	説明
ユーザ名	セッション レコードのユーザ名。ユーザ設定を表示するには、ユーザ名をクリックします。
IP	ユーザが IoT FND にアクセスするために使用するシステムの IP アドレス。
Login Time	ユーザのログイン日付および時刻。
Last Access Time	ユーザがシステムに前回アクセスした時刻。

ヒント：ユーザ リストを更新するには、[Refresh] をクリックします。

Logging Users Out

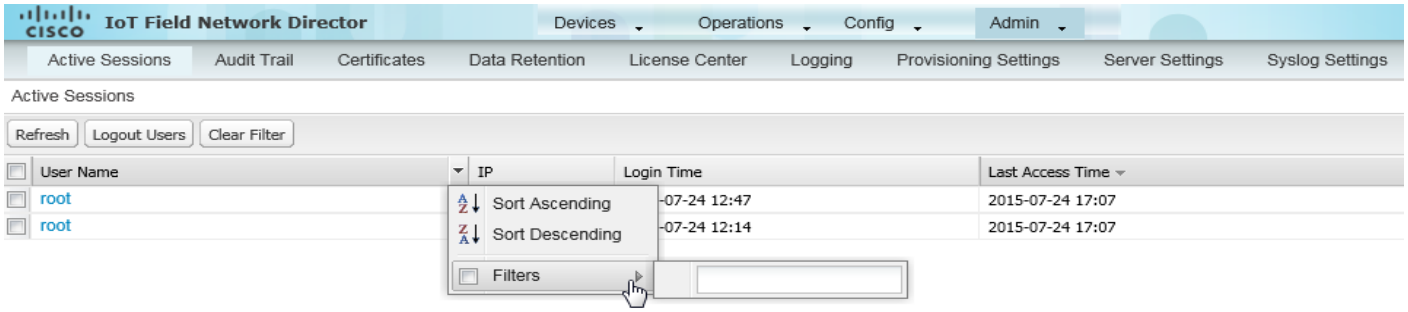
IoT FND ユーザをログアウトさせるには、次の手順を実行します。

1. [Admin] > [System Management] > [Active Sessions] を選択します。
2. ログアウトするユーザのチェックボックスをオンにします。
3. [Logout Users] をクリックします。
4. [Yes] をクリックします。

アクティブ セッション リストのフィルタリング

[Active Sessions] リストをカラム フィルタを使用してフィルタリングするには、次の手順を実行します。

1. [Admin] > [System Management] > [Active Sessions] を選択します。
2. [User Name] ドロップダウン メニューから、[Filters] を選択して、ユーザ名を入力するか、ユーザ名の最初の文字を入力してリストをフィルタリングします。



たとえば、root ユーザのアクティブ セッションをリストするには、**root** と入力します。

ヒント：フィルタを削除するには、[User Name] ドロップダウン メニューで [Filters] チェックボックスをオフにし、[Clear Filter] をオンにします。

監査証跡の表示

監査証跡を使用して、IoT Field Network Director のユーザ アクティビティを追跡します。

監査証跡を表示するには、[Admin] > [System Management] > [Audit Trail] を選択します。

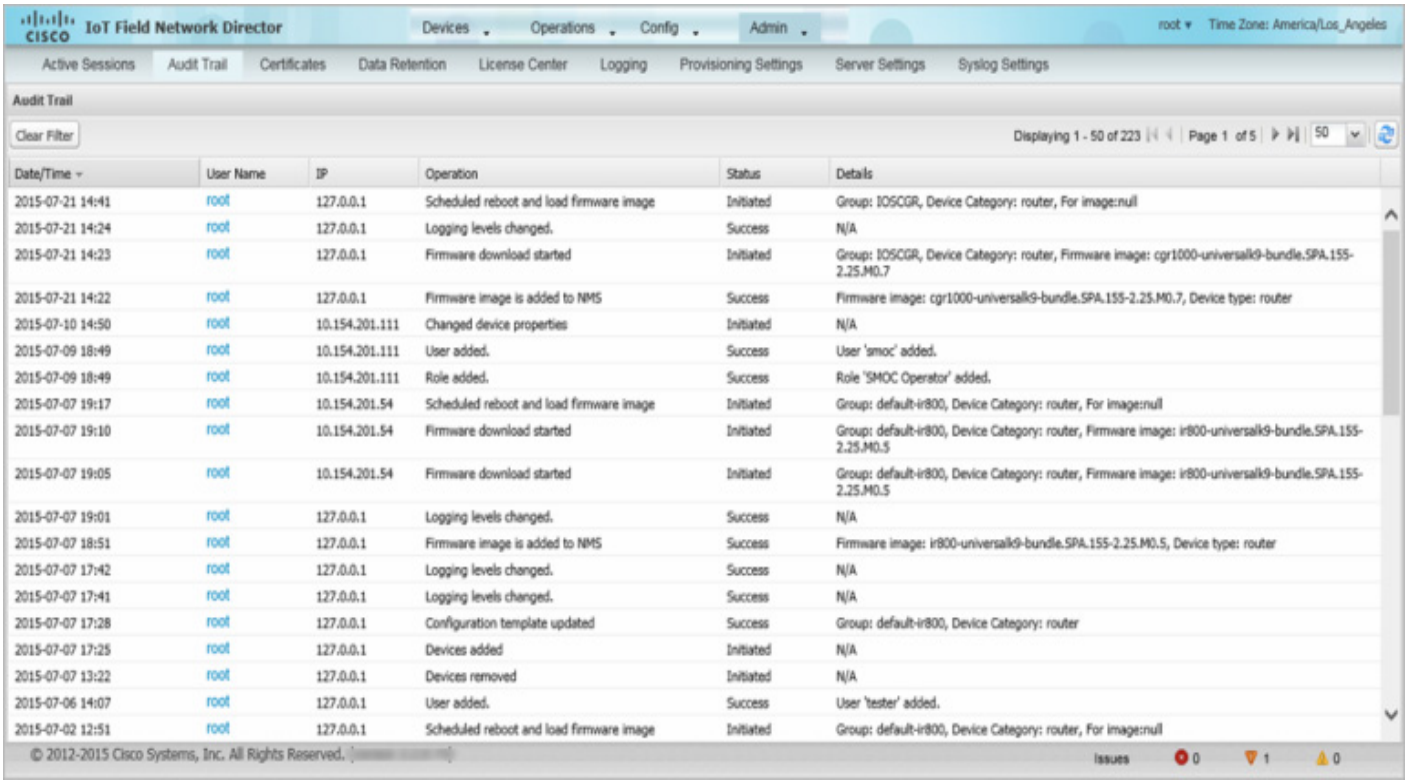


表 2 は、監査証跡のフィールドを説明しています。

表 2　監査証跡のフィールド

フィールド	説明
Date/Time	操作の日付と時刻。
ユーザ名	操作を実行したユーザ。ユーザ設定を表示するには、ユーザ名をクリックします。
IP	ユーザが IoT FND にアクセスするために使用するシステムの IP アドレス。
動作	実行された操作の種類。
Status（ステータス）	操作のステータス。
詳細	操作の詳細。

ヒント: リストを更新するには、[Refresh] をクリックします。

監査証跡リストのフィルタリング

[Audit Trail] リストをカラム フィルタを使用してフィルタリングするには、次の手順を実行します。

1. [Admin] > [System Management] > [Audit Trail] を選択します。
2. [User Name] ドロップダウン メニューから、[Filters] を選択して、ユーザ名を入力するか、ユーザ名の最初の文字を入力してリストをフィルタリングします。

   たとえば、ユーザ jane の監査証跡エントリを表示するには、**jane** と入力します。

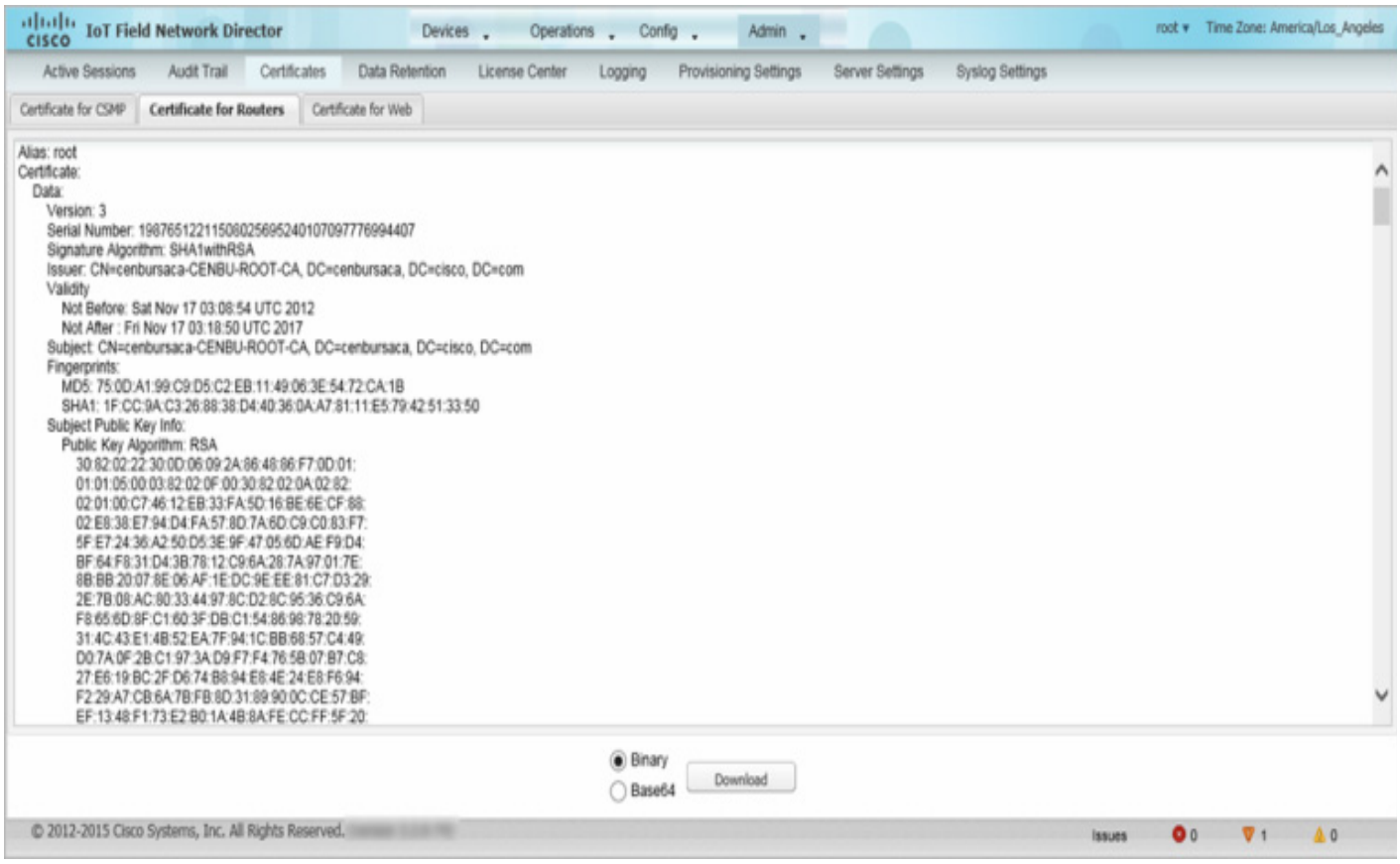
   ヒント: フィルタを削除するには、[User Name] ドロップダウン メニューで [Filters] チェックボックスをオフにし、[Clear Filter] をオンにします。

証明書の管理

[Certificates] ページには、CSMP（CoAP Simple Management Protocol）、IoT-DM（IoT Device Manager）、および IoT FND が使用する Web のそれぞれに対する証明書が表示され、それらの証明書をダウンロードできます。

CSMP、IoT-DM、および Web 証明書を表示するには、次の手順を実行します。

1. [Admin] > [System Management] > [Certificates] を選択します。
2. 証明書を表示するには、対応するタブをクリックします。



3. 証明書をダウンロードするには、エンコーディング（[Binary] または [Base64]）ラジオ ボタンをクリックし、[Download] をクリックします。

証明書の詳細については、証明書の生成およびインストールを参照してください。

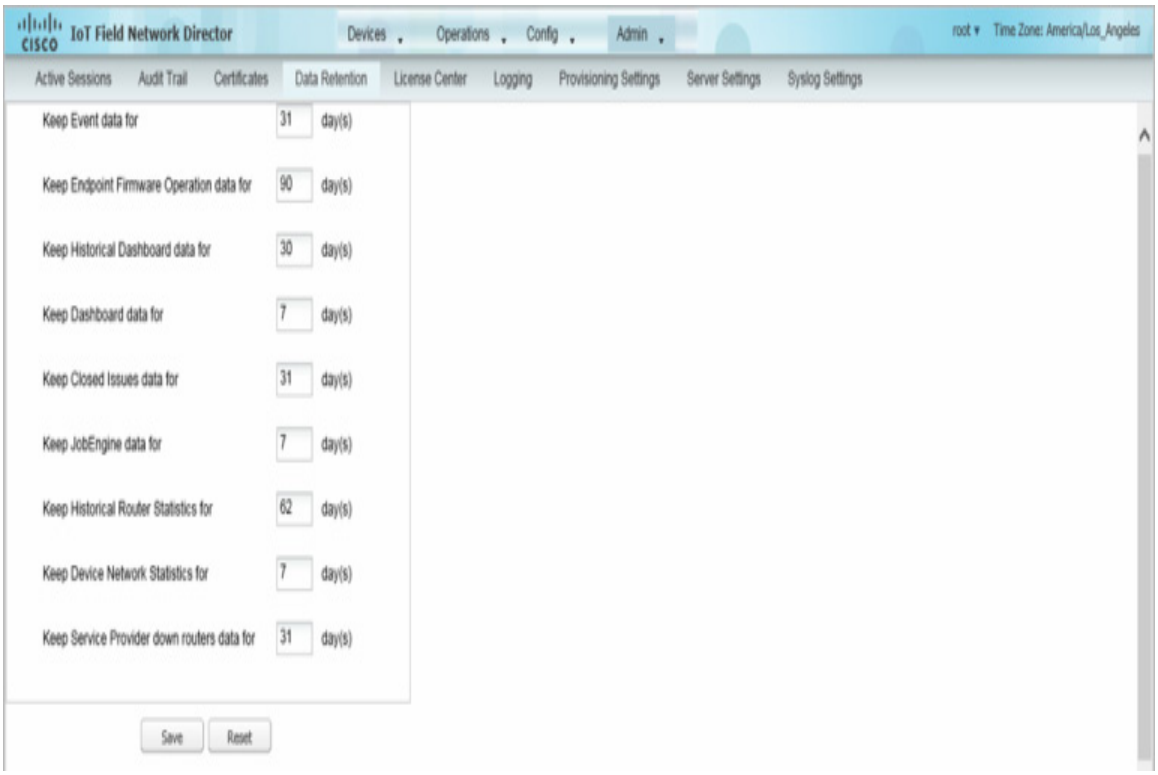
データ保存の設定

[Data Retention] ページでは、IoT FND データベースにイベント、問題、およびメトリック データを保持する日数を決定することができます。

（注）データ保持では、イベントが未解決の問題に関連付けられている場合でもイベントを切り取ります。

IoT FND データ保持を設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Data Retention] を選択します。



2. それぞれの保持カテゴリに、データを保持する日数を指定します。

   表 3 は、各フィールドの許容最大値をリストしています。

表 3　　データ保持フィールドの許容最大値

フィールド	日数の値		
	最小ハードウェア	最大	デフォルト
イベント データ	1	90	31
Firmware data	7	180	7
Historical NMS data	1	90	62
NMS data	1	7	7
Closed issues data	1	90	30
Job engine data	1	30	30
Historical router data	1	90	30
Device data	1	7	7
Service provider down routers data	1	31	31

3. [Save（保存）] をクリックします。
4. デフォルト設定に戻すには、[Reset] をクリックします。

ライセンスの管理

[License Center] ページ（[Admin] > [System Management] > [License Center]）で、ライセンス ファイルを表示および管理できます。

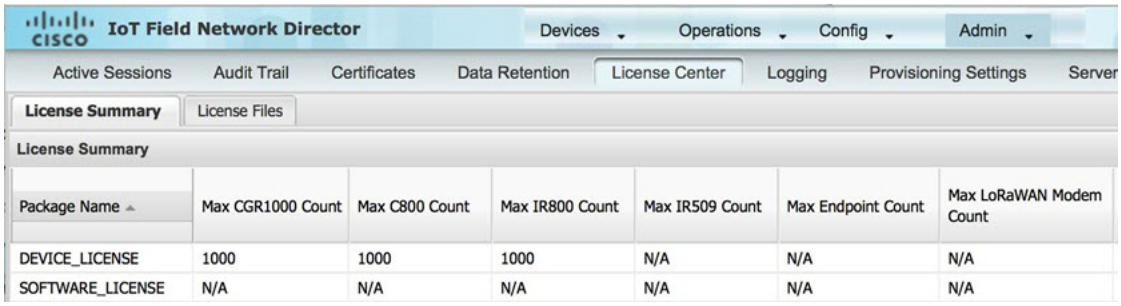
- ライセンス概要の表示
- ライセンス ファイルの表示
- ライセンス ファイル詳細の表示
- ライセンス ファイルの追加
- ライセンス ファイルの削除

（注）IoT FND は、デバイスのインポート時にライセンスの適用を実行します。ライセンスがない場合には、IoT FND は 3 つの FAR と 100 のメッシュ エンドポイントのみを許可します。ライセンスを追加すると、IoT FND では、ライセンスで定義されている、許可された数のデバイスしかインポートできなくなります。

ライセンス概要の表示

IoT FND ライセンスの概要を表示するには、次の手順を実行します。

1. [Admin] > [System Management] > [License Center] を選択します。
2. [License Summary] をクリックします。



すべてのライセンスについて、IoT FND は、表 4 で説明されている情報を表示します。

（注）IR500 は、メッシュ エンドポイント ライセンスを使用し、特別なライセンスは不要です。

表 4　ライセンス ファイル情報

フィールド	説明
Package Name	ライセンス パッケージの数。
Max CGR1000 Count	サポートされる CGR 1000 の最大数。
Max C800 Count	サポートされる C800 デバイスの最大数。
Max IR800 Count	サポートされる IR809 および IR829 デバイスの最大数。
Max IR509 Count	サポートされる IR500 デバイスの最大数。
Max Endpoint Count	サポートされるメッシュ エンドポイントの最大数。
Max LoRaWAN Modem Count	サポートされる LoRaWAN モデム（モジュール）の最大数。

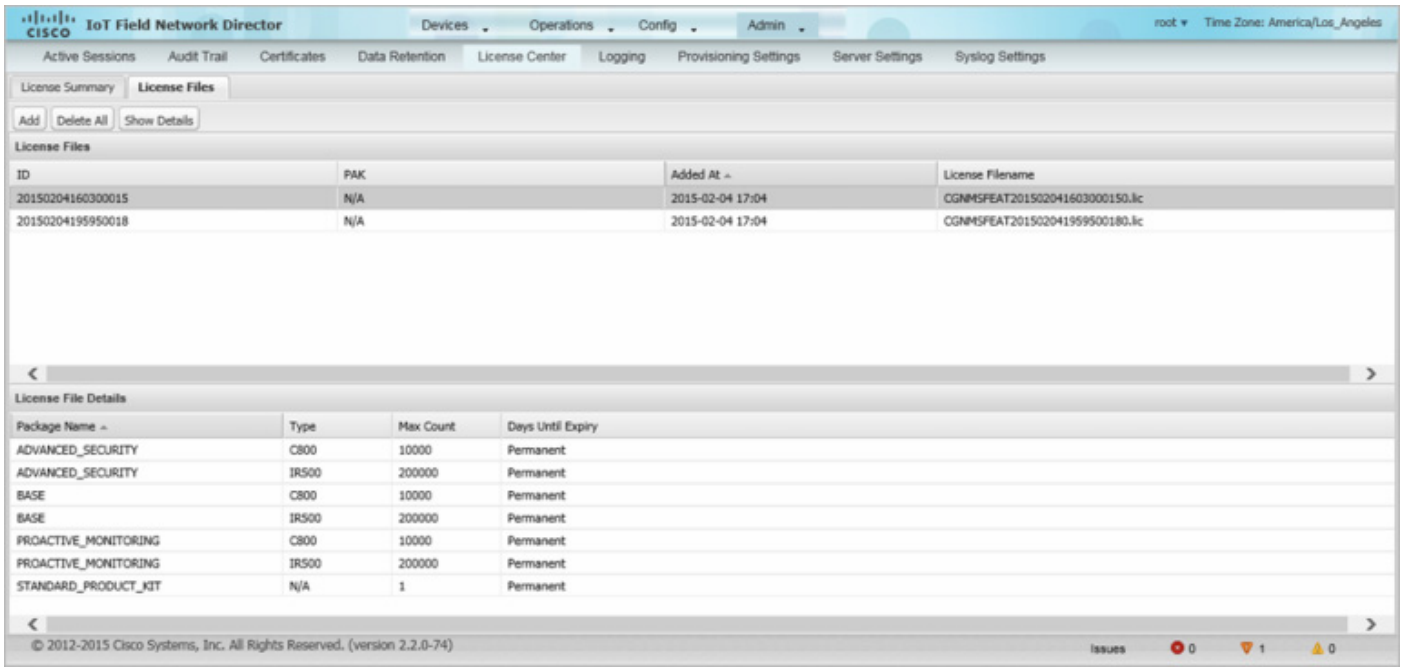
表 4　ライセンス ファイル情報（続き）

フィールド	説明
Max User	サポートされるユーザの最大数。
Max NBAPI User	サポートされる IoT FND North Bound API ユーザの最大数。
Days Until Expiry	ライセンスの有効期限が切れるまでの残りの日数。

ライセンス ファイルの表示

IoT FND ライセンス ファイルを表示するには、次の手順を実行します。

1. [Admin] > [System Management] > [License Center] を選択します。
2. [License Files] をクリックします。



すべてのファイルについて、IoT FND は、表 5 で説明されているフィールドを表示します。

表 5　ライセンス ファイルのフィールド

フィールド	説明
ID	ライセンス ID。
PAK	ライセンス履行の発行数。
Added At	ライセンスが IoT FND に追加された日付と時刻。
License Filename	ライセンスのファイル名。

ライセンス ファイル詳細の表示

ライセンス ファイル詳細を表示するには、次の手順を実行します。

1. [Admin] > [System Management] > [License Center] を選択します。
2. [License Files] をクリックします。

3. 表示するライセンスを選択します。
4. [Show Details] をクリックします。

   選択したすべてのファイルについて、[License File Details] セクションに次の情報が表示されます。

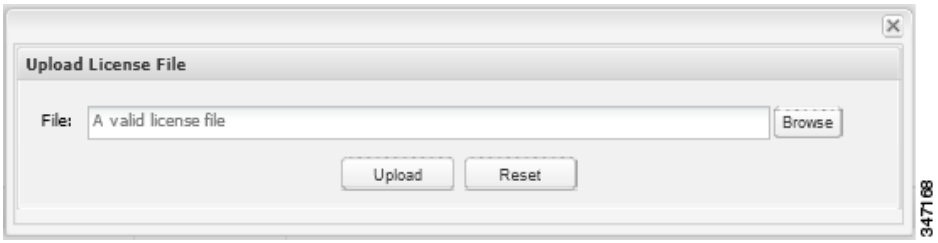
表 6　　ライセンス ファイル詳細

フィールド	説明
Package Name	ライセンス パッケージ名です。
タイプ	ライセンス ターゲット（ROUTER、ENDPOINT、USER、NB_USER）。タイプは、値が適切でない場合の空の文字列です。
Max Count	このライセンスの対象となるターゲット デバイスの最大数。
Days Until Expiry	ライセンスの期限が切れるまでの残りの日数。

ライセンス ファイルの追加

ライセンス ファイルを追加するには、次の手順を実行します。

1. [Admin] > [System Management] > [License Center] を選択します。
2. [License Files] をクリックします。
3. [Add] をクリックします。



4. [Browse] をクリックし、ライセンス ファイルを見つけて、[Open] をクリックします。
5. [Upload] をクリックします。

ライセンス ファイルの削除

(注)すべてのライセンス ファイルは、削除可能です。既存のライセンス ファイルを削除する前に、ライセンス ファイルにアクセスできることを確認します。ライセンスがない場合には、IoT FND は 3 つの FAR と 100 のメッシュ エンドポイントの登録のみを許可します。

ライセンス ファイルを削除するには、次の手順を実行します。

1. [Admin] > [System Management] > [License Center] を選択します。
2. [License Files] をクリックします。
3. [Delete All] をクリックし、[Yes] をクリックします。

ログの管理

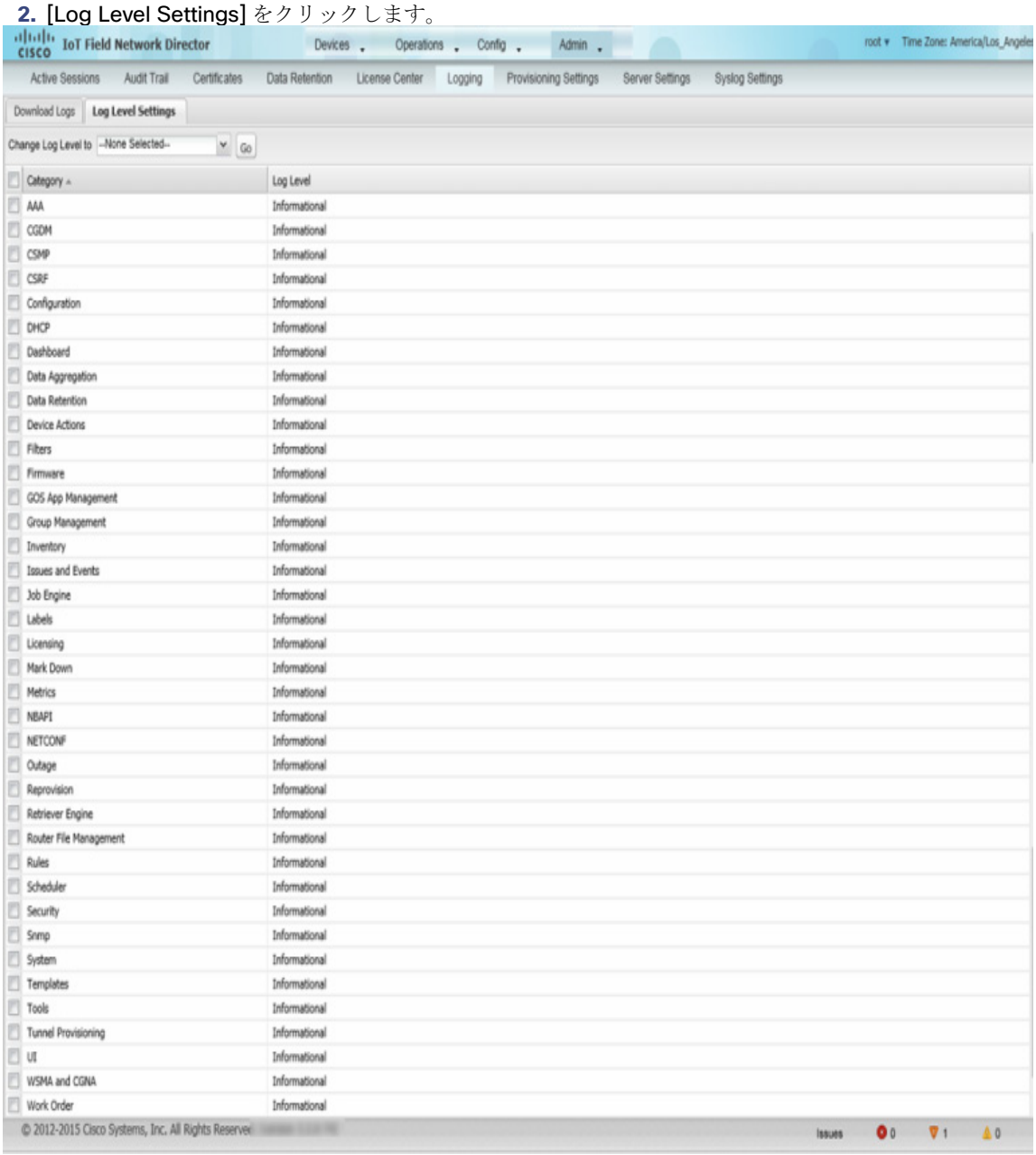
- ログの設定
- ログのダウンロード

ログの設定

IoT FND により、さまざまなログ カテゴリのログ レベルを変更したり、ログをダウンロードしたりできます。ログはある程度の量のディスク スペースを占めます。たとえば、500 万個のメーターが 8 時間のレポート間隔に設定されており、5000 のルータが 60 分の定期インベントリ通知に設定されている場合には、ディスク消費量はおよそ 7 MB/秒になります。サーバにログを保持する十分なディスク スペースがあることを確認します。

ログ レベルを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Logging] を選択します。
2. [Log Level Settings] をクリックします。



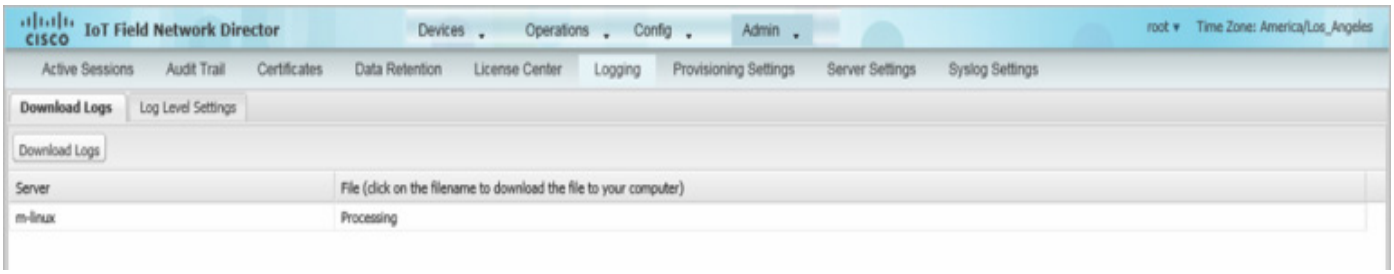
3. 設定するすべてのログ カテゴリのチェックボックスをオンにします。
4. [Change Log Level to] ドロップダウン メニューから、ログ レベルの設定（[Debug] または [Informational]）を選択します。
   - 表示可能なすべてのロギング メッセージを生成するには、[Debug] レベルを使用します。
     （注）[Debug] ログ カテゴリを実行すると、パフォーマンスに影響を与える可能性があります。
   - これらのメッセージのサブセットを生成するには、[Informational] ログ レベルを使用します。
     （注）[Informational] ログ レベルは、IoT FND が開いている場合はすべてのカテゴリのデフォルトです。カスタム ログ レベルの設定は、複数のログイン セッションにわたって保持されますが、IoT FND の再起動後には保持されません。
5. 設定を適用するには、[Go] をクリックします。

   （注）server.log ファイルは、サイズに基づいてローテーションされます。

ログのダウンロード

ログをダウンロードするには、次の手順を実行します。

1. [Admin] > [System Management] > [Logging] を選択します。
2. [Download Logs] タブをクリックします。



3. [Download Logs] ボタンをクリックします。
   - シングルサーバ導入システムでこのボタンをクリックすると、IoT FND はログ ファイルを単一の zip ファイルに圧縮し、[Download Logs] ペインに項目とその zip ファイルへのリンクを追加します。
   - IoT FND クラスタ導入環境では、このボタンをクリックすると、接続先の IoT FND サーバが次のことを行います。
     - サーバ上の複数のログ ファイルを単一の zip ファイルに圧縮し、[Download Logs] ペインに項目とその zip ファイルへのリンクを追加します。
     - 他のサーバからこのサーバへの .zip 形式でのログ ファイルの転送を開始します。ファイルが使用可能になると、サーバはこれらのファイルの項目を [Download Logs] ペインに追加します。
4. zip ファイルをローカルにダウンロードするには、そのファイル名をクリックします。

ヒント：クラスタ環境では、ログ ファイルをシスコサポートに送信する必要がある場合には、必ずすべてのクラスタ サーバのログファイルを送信してください。

プロビジョニングの設定

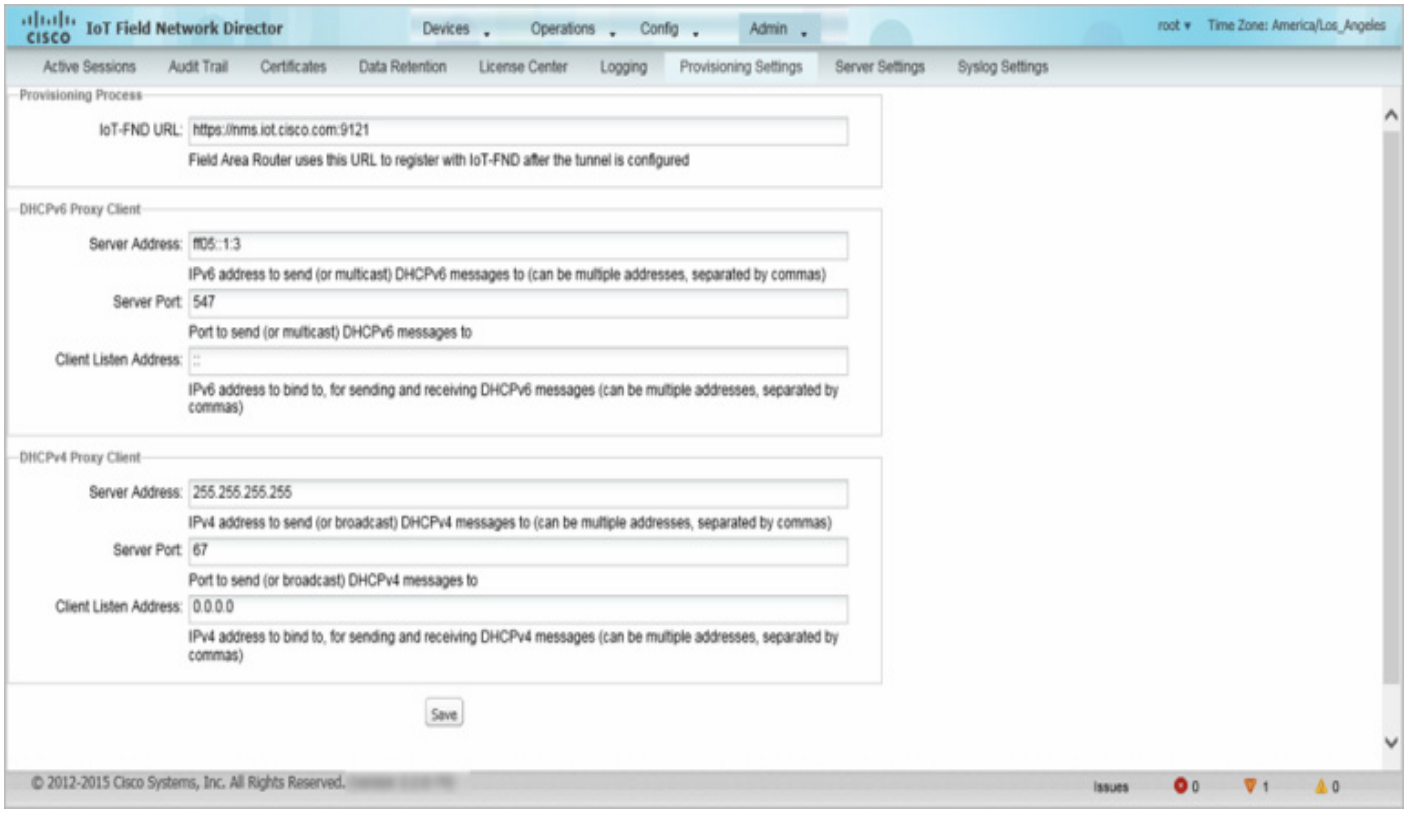
[Provisioning Settings] ページ（[Admin] > [System Management] > [Provisioning Settings]）では、IoT FND が FAR と ASR との間にトンネルを作成するために必要な、IoT FND の URL、DHCPv4 プロキシ クライアント、および DHCPv6 プロキシ クライアントの設定を行うことができます（図 3）。IoT FND アーキテクチャで使用されるトンネルの例については、図 1 を参照してください。トンネルのプロビジョニングについては、トンネル プロビジョニング設定プロセスを参照してください。さらに、ZTD 中には、DHCP コールをリース IP アドレスのデバイス設定テンプレートに追加できます。

(注) Red Hat Linux 7.x サーバ インストール システムの場合、特定の IPv4 および IPv6 アドレスを、IoT FND Linux ホスト サーバから DHCP IPv4 および IPv6 クライアントのバインド先に、IoT FND で次の値を設定して構成する必要があります。

- [Admin] > [Provisioning Settings] > [DHCPv6 Proxy Client] > [Client Listen Address]：IPv6 DHCP リースを DHCP サーバから取得するために使用するインターフェイスの IPv6 アドレスに値を設定します。デフォルト値は「::」です デフォルト設定を、Linux ホスト マシンの実際の IPv6 アドレスに変更します。
- [Admin] > [Provisioning Settings] > [DHCPv4 Proxy Client] > [Client Listen Address]：IPv4 DHCP リースを DHCP サーバから取得するために使用するインターフェイスの IPv4 アドレスに値を設定します。デフォルト値は「0.0.0.0」です。デフォルト設定を、Linux ホスト マシンの実際の IPv4 アドレスに変更します。

(注) トンネルとプロキシの設定を構成するには、root としてログインするか、または管理操作権限を持つユーザとしてログインする必要があります。

図 3　[Provisioning Settings] ページ



この項では、トンネル設定を構成するための次のトピックを記載しています。

- IoT FND サーバ URL の設定
- DHCPv6 プロキシ クライアントの設定
- DHCPv4 プロキシ クライアントの設定

IoT FND サーバ URL の設定

IoT FND URL は、トンネルの確立後に FAR が IoT FND のアクセスに使用する URL です。この URL は、定期的なインベントリの間にもアクセスされます。ZTD 中に、FAR は TPS プロキシを経由した IoT FND へのアクセスからこの URL の使用へと移行しますが、これはトンネルを経由した使用に適している必要があります。

IoT FND URL を設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Provisioning Settings] を選択します。
2. [IoT FND URL] フィールドに、IoT FND サーバの URL を入力します。

   この URL は、HTTPS プロトコルを使用する必要があり、登録要求を受信するために指定されているポート番号を含める必要があります。デフォルトでは、ポート番号は 9121 です。次に例を示します。

   ```
   https://nms.sgbu.example.com:9121
   ```

3. [Save（保存）] をクリックします。

DHCPv6 プロキシ クライアントの設定

DHCPv6 プロキシ クライアントを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Provisioning Settings] を選択します。
2. DHCPv6 プロキシ クライアントの設定:

   a. [Server Address] フィールドに、トンネル IP アドレスを指定する DHCPv6 サーバのアドレスを入力します。

   複数のアドレスをカンマで区切って入力することもできます。ただし、たいていの場合は、1 つのサーバで間に合います。IoT FND は、DHCP プロトコルを使用してトンネル IP アドレスを取得しようとします。取得できない場合は、リスト内の次のサーバに移動して試行を繰り返します。

   b. [Server Port] フィールドで、DHCPv6 要求を送信する DHCP サーバのポート アドレスを入力します。

   (注) DHCP サーバを非標準ポートで動作するように設定したのない限り、デフォルトのポート番号（547）は変更しないでください。

   c. [Client Listen Address] フィールドに、DHCPv6 メッセージを送受信するためにバインドするアドレスを入力します。

   これは、DHCP サーバが IoT FND と通信するために使用するインターフェイスのアドレスです。複数のバックアップ アドレスをカンマで区切って入力できます。

   ヒント：ホストに複数のインターフェイスがある IoT FND インストール システムの場合、クライアントはリストされている各発信元アドレスを使用して要求を送信します。デフォルト値「0.0.0.0」（IPv4）および「::」（IPv6）では、クライアントは各インターフェイスに要求を送信します。通常、1 つのインターフェイスが DHCP サーバに接続します。これらのインストール システムで、[Client Listen Address] フィールドをアクセスするインターフェイスの IP アドレスに設定すると、すべてのクライアント要求がそのインターフェイスに送信されます。

3. [Save（保存）] をクリックします。

DHCPv4 プロキシ クライアントの設定

DHCPv4 プロキシ クライアントを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Provisioning Settings] を選択します。
2. DHCPv4 プロキシ クライアントの設定:

a. [Server Address] フィールドに、トンネル IP アドレスを指定する DHCPv4 サーバのアドレスを入力します。

複数のアドレスをカンマで区切って入力することもできます。ただし、たいていの場合は、1 つのサーバで間に合います。IoT FND は、トンネル IP アドレスをリスト内の先頭のサーバから取得しようとします。取得できない場合は、リスト内の次のサーバに移動して試行を繰り返します。

b. [Server Port] フィールドで、DHCPv4 要求を送信する DHCP サーバのポート アドレスを入力します。

(注) DHCP サーバを非標準ポートで動作するように設定していない限り、デフォルトのポート番号(67)は変更しないでください。

c. [Client Listen Address] フィールドに、DHCPv4 メッセージを送受信するためにバインドするアドレスを入力します。

これは、DHCP サーバが IoT FND と通信するために使用するインターフェイスのアドレスです。複数のバックアップ アドレスをカンマで区切って入力できます。

3. [Save(保存)] をクリックします。

サーバ設定値の設定

[Server Settings] ページ([Admin] > [System Management] > [Server Settings])では、サーバ設定を表示および管理できます。

- ダウンロード ログの設定
- Web セッションの設定
- [Device Down Timeouts] の設定
- 請求期間の設定
- RPL ツリー ポーリングの設定
- [Issue] ステータス バーの設定

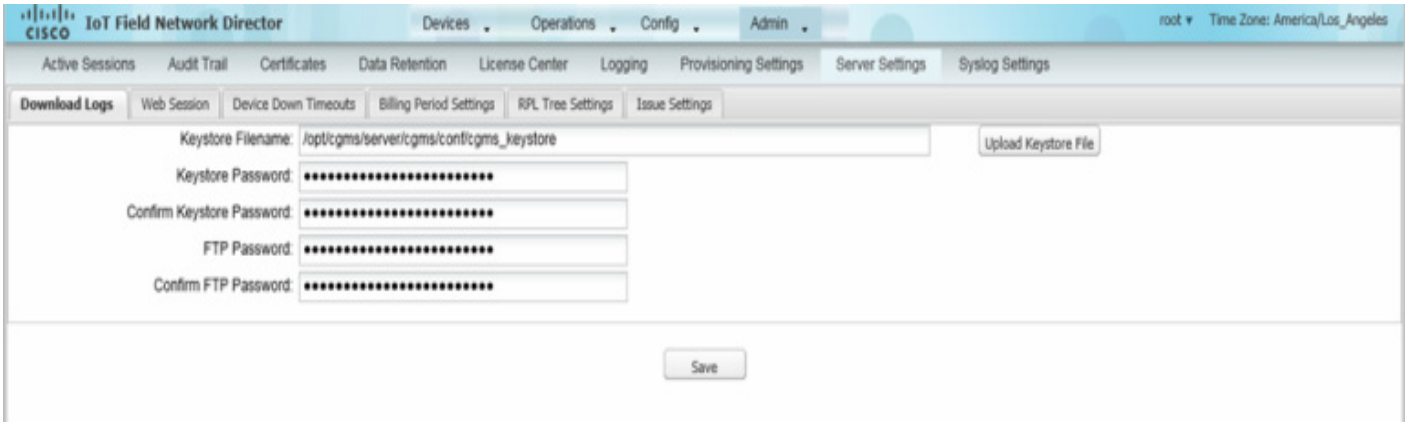
ダウンロード ログの設定

(注) ダウンロード ログの設定は、IoT FND クラスタをセットアップする場合にのみ必要です。

[Download Logs] ページでは、キーストア設定を行うことができます。

ダウンロード ログを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Server Settings] を選択します。
2. [Download Logs] タブをクリックします。



3. 設定する項目は次のとおりです。

表 7　　キーストア設定

フィールド	説明
キーストアのファイル名	[Upload Keystore File] をクリックして、キーストア ファイルを、IoT FND が使用する X.509 証明書の公開キーでアップロードします。同じキーストア ファイルを再利用できます。
Keystore Password	IoT FND が起動時にキーストア ファイルにアクセスするために使用するパスワードを入力します。
Confirm Keystore Password	
FTP パスワード	FTP パスワードを入力します。
Confirm FTP Password	

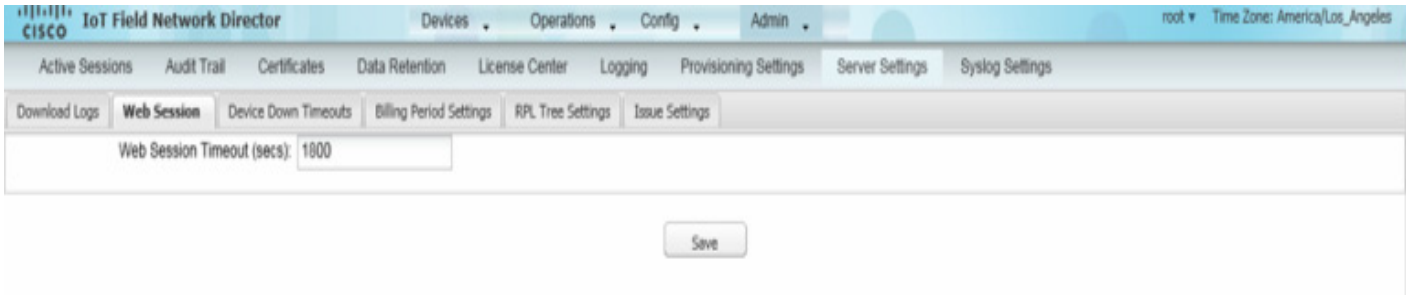
4. [Save（保存）] をクリックします。

Web セッションの設定

[Web Sessions] ページでは、経過すると IoT FND が Web セッションを終了してユーザをログアウトするタイムアウト秒数を指定できます。

Web セッション タイムアウトを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Server Settings] を選択します。
2. [Web Session] タブをクリックします。



3. タイムアウト秒数を入力します。有効値の範囲は 0 ～ 86400（24 時間）です。

   Web セッションが指定された長さの期間、アイドル状態であれば、IoT FND はセッションを終了し、ユーザをログアウトします。

4. [Save（保存）] をクリックします。

[Device Down Timeouts] の設定

[Device Down Timeouts] ページでは、経過すると IoT FND でルータ（ASR、FAR）とエンドポイントのステータスが *Down* に変更されるタイムアウト秒数を指定できます。デバイスのダウン ポーリング間隔は 5 分です。システムは、デバイス ダウン タイムアウト値と最終登録時間を使用して、デバイス ステータスを Down に変更するかどうかを決定します。たとえば、FAR デバイスのダウン タイムアウト値が 2 時間（7200 秒）に設定されている場合、最終 heard 時間が 2 時間よりも前であるすべての FAR は、ステータスが Down とマークされます。

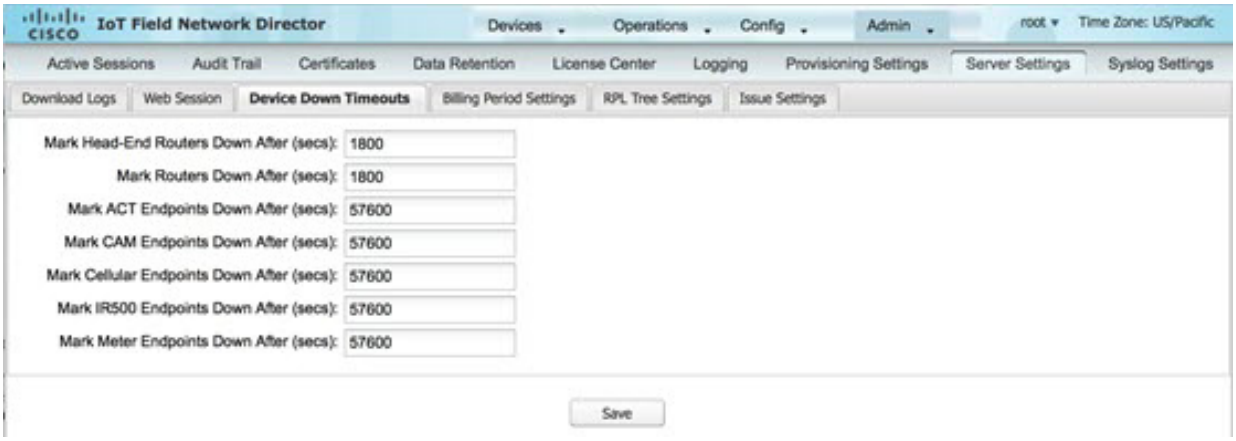
さらに、FAR 設定グループとエンドポイント設定グループに対してデバイス タイムアウト設定を指定することもできます。

デバイス ステータスは、IoT FND が次のいずれかを検出すると Up に変更されます。

- 定期的なインベントリ通知
- Event
- 手動メトリック更新
- デバイス登録

デバイスのダウン タイムアウト設定を構成するには、次の手順を実行します。

1. [Admin] > [System Management] > [Server Settings] を選択します。
2. [Device Down Timeouts] タブをクリックします。



3. リストされている各デバイス タイプに対して、経過するとデバイスのステータスが IoT FND で Down に変更される秒数を入力します。

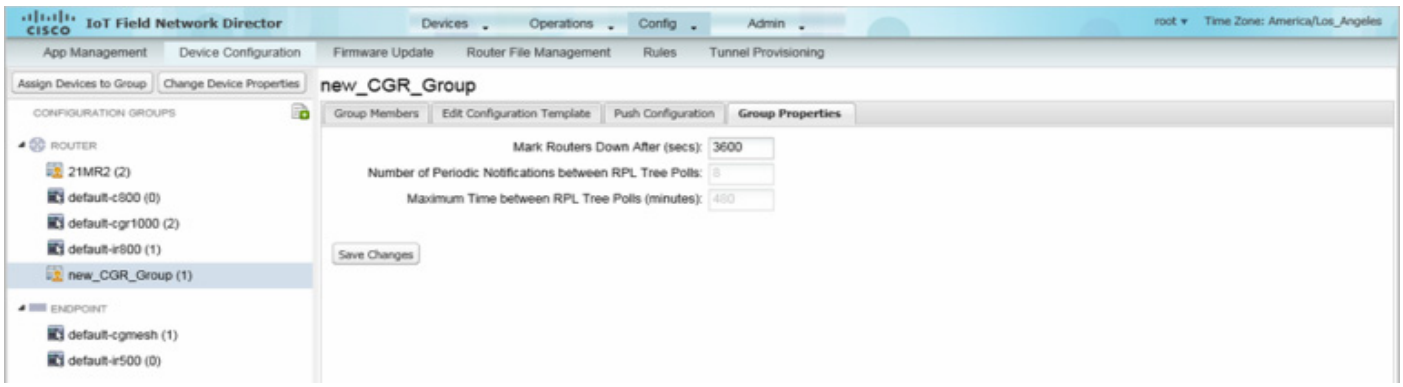
   値は対応するポーリング間隔より大きくなければなりません。たとえば、エンドポイントのデフォルトのポーリング間隔は 8 時間（28800 秒）であるため、[Mark Mesh Endpoints Down After (secs)] フィールドの値には、28800 より大きい数値を指定する必要があります。

4. [Save（保存）] をクリックします。

FAR 設定グループとエンドポイント設定グループに対するデバイス ダウン タイムアウト設定

FAR 設定グループまたはエンドポイント設定グループにデバイス ダウン タイムアウト設定を指定するには、次の手順を実行します。

1. [Config] > [Device Configuration] を選択します。
2. 左側ペインで、[ROUTERS] または [ENDPOINTS] を設定するデバイスを選択します。
3. [Group Properties] タブをクリックします。



4. [Mark Routers Down After (secs)] または [Mark Endpoints Down After (secs)] フィールドに、IoT FND でグループ内のデバイス(ルータまたはエンドポイント)のステータスが、経過すると Down に変更される秒数を入力します。

   値は対応するポーリング間隔より大きくなければなりません。

   たとえば、FAR のデフォルトのポーリング間隔は 30 分(1800 秒)であるため、[Mark Routers Down After (secs)] フィールドの値には、1800 より大きい数値を指定する必要があります。

   FAR のデフォルトのポーリング間隔は 960 分(57600 秒)であるため、[Mark Routers Down After (secs)] フィールドの値には、57600 秒より大きい数値を指定する必要があります。

5. [Save Changes] をクリックします。

請求期間の設定

IoT FND では、セルラーおよびイーサネット(サテライト)サービスの、月次請求期間の開始日を設定できます。

請求期間の設定を行うには、次の手順を実行します。

1. [Admin] > [System Management] > [Server Settings] を選択します。
2. [Billing Period Settings] タブをクリックします。

3. セルラーとイーサネットの請求期間の開始日を入力します。
4. ドロップダウン メニューから、請求期間のタイム ゾーンを選択します。
5. [Save(保存)] をクリックします。

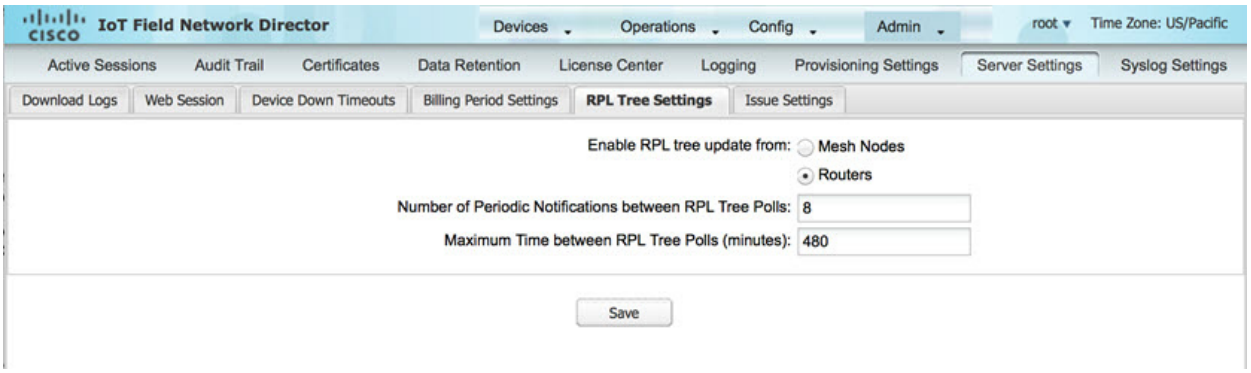
RPL ツリー ポーリングの設定

RPL ツリー ポーリングは、FAR 定期通知イベントから派生します。RPL ツリーは FAR から定期通知イベントでプッシュされることはないので、IoT FND は設定された間隔で RPL ツリーを明示的にポーリングする必要があります。IoT FND では、RPL ツリー ポーリング サイクル(つまり、次の RPL ツリー ポーリングまでに実行される定期通知イベント回数)と、ツリー ポーリングの間の最大時間を設定できます。

注意: CG-NMS 1.1(5) リリースは、ルータ RPL ツリーの更新をサポートしていません。ルータからの RPL ツリーの更新は有効にしないでください。

RPL ツリー ポーリングを設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Server Settings] を選択します。
2. [RPL Tree Settings] タブを選択します。



3. メッシュ ノードまたは CGR デバイスに対して [Enable RPL tree update from] ラジオ ボタンを選択し、指定された間隔でそれらのデバイスから RPL ツリー更新を受け取るようにします。
4. ルータのポーリングの場合は、RPL ツリー ポーリング間隔の間に受け渡すイベントの数を、[Number of Periodic Notification RPL Tree Polls] フィールドに入力します。
   - デフォルト値は 8 です。

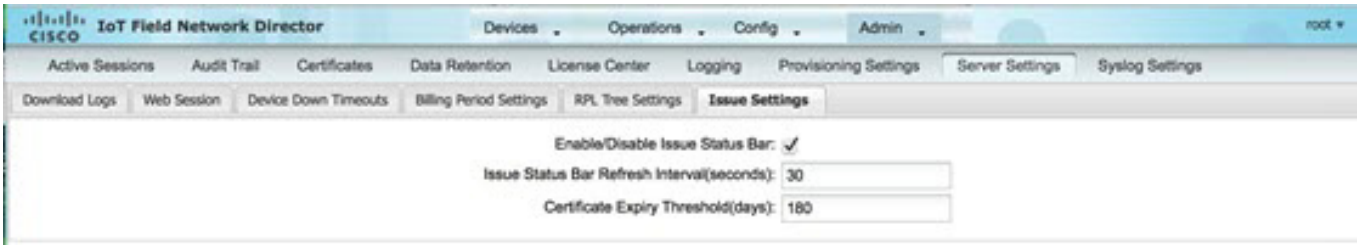
     (注) 定期通知イベントの間にしきい値を上回った場合、IoT FND は RPL ツリー ポーリングを実行します。
5. [Maximum Time between RPL Tree Polling (minutes)] フィールドに、ツリー ポーリングの間の最大期間を分単位で入力します。
   - デフォルト値は 480 分(8 時間)です。
6. [Save(保存)] をクリックします。

[Issue] ステータス バーの設定

[Issue] ステータス バーには、デバイス タイプごとの問題が表示され(ユーザ設定に従います:ユーザ プリファレンスの設定を参照)、左下のブラウザ フレームには重大度レベルが示されます。

[Issue] ステータス バーを有効にして、更新間隔を設定するには、次の手順を実行します。

1. [Choose Admin] > [System Management] > [Sever Settings] > [Issue Settings] を選択します。



2. ブラウザ フレームに [Issue] ステータス バーを表示するには、[Enable/Disable Issue Status Bar] チェックボックスをオンにします。
3. [Issue Status Bar Refresh Interval] フィールドに、更新値を秒単位で入力します。
   - 有効な値は、30(デフォルト)～ 300 秒(5 分)です。

4. サポート対象のすべてのルータまたは IoT FND アプリケーション サーバに対して、[Certificate Expiry Threshold (days)] フィールドに日数の値を入力します。
   - 有効な値は、180（デフォルト）～ 365 日です。

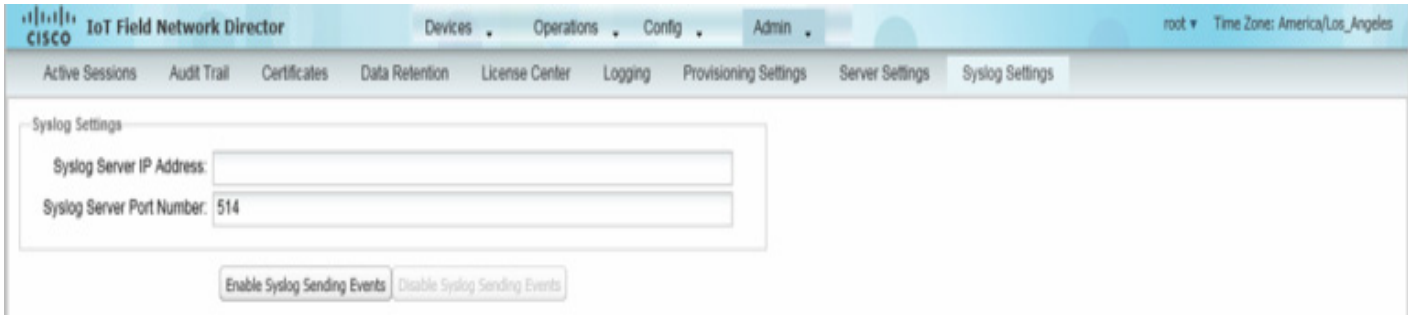
（注）設定された [Certificate Expiry Threshold] のデフォルト日数に達すると、Major イベントである certificateExpiration が生成されます。証明書の有効期限が切れると（180 日より長い）、Critical イベントである certificateExpired が作成されます。

Syslog の管理

IoT FND は、デバイス イベントを受信すると、そのデータベース内に保存して、Syslog メッセージをサードパーティ アプリケーションの統合が可能な Syslog サーバに送信します。

Syslog 転送を設定するには、次の手順を実行します。

1. [Admin] > [System Management] > [Syslog Settings] を選択します。



2. [Syslog Server IP Address] フィールドに、Syslog サーバの IP アドレスを入力します。
3. [Syslog Server Port Number] フィールドで、デバイス イベントを受け取るポート番号を入力します（デフォルトは 514）。
   - Syslog サーバへのメッセージ転送を有効にするには、[Enable Syslog Sending Events] をクリックします。
   - Syslog サーバへのメッセージ転送を無効にするには、[Disable Syslog Sending Events] をクリックします。

IoT FND クラスタ ソリューションの場合、クラスタ内の各サーバはイベントを同じ Syslog サーバに送信します。

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。

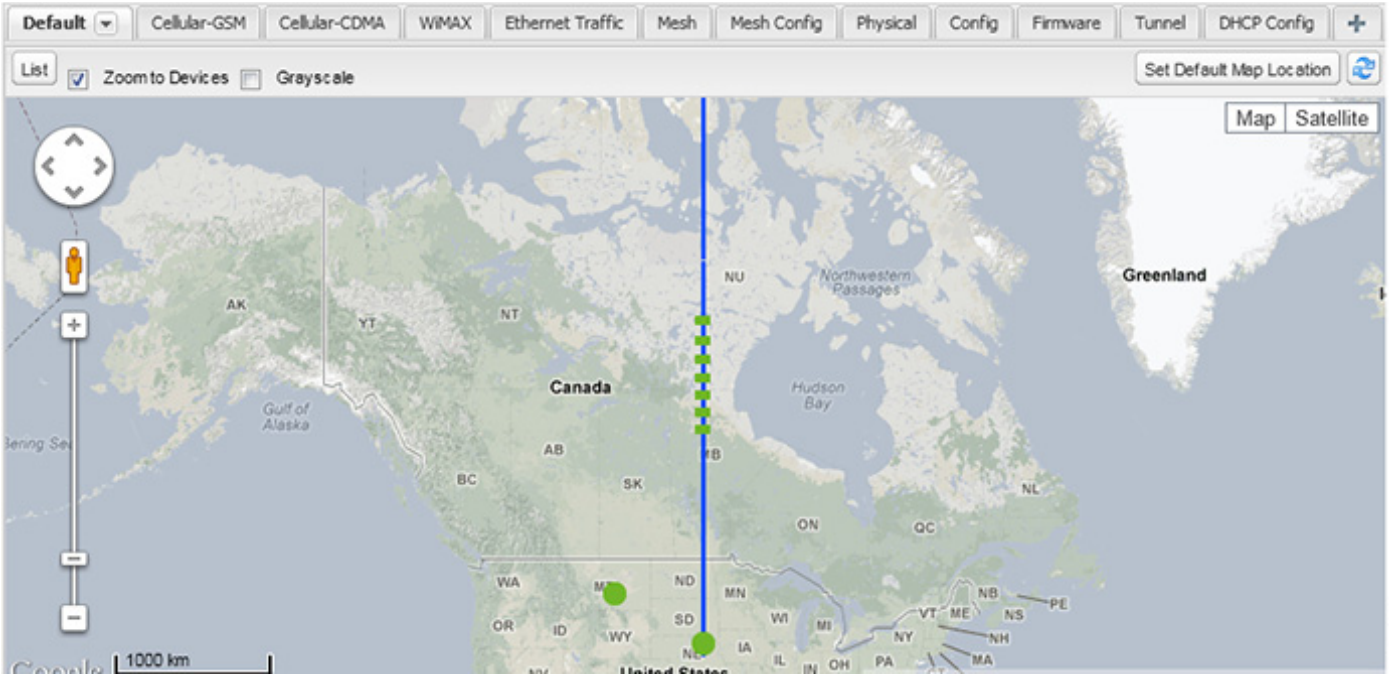
これらのビューで実行する共通アクション(たとえば、ラベルの追加やデバイス プロパティの変更)の詳細については、「共通のデバイス操作」を参照してください。

[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

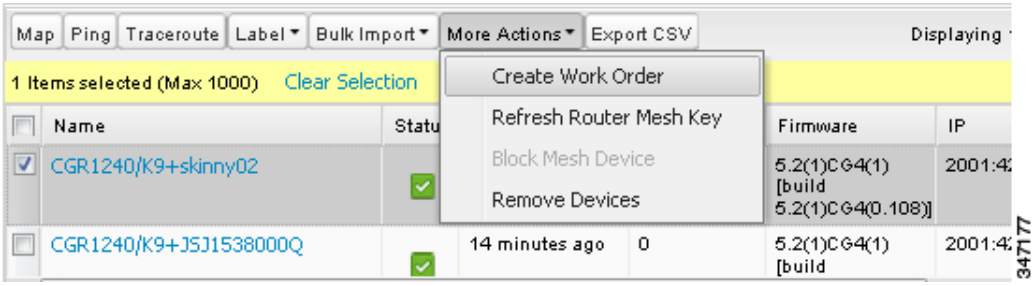
デバイス検査のためにフィールド技術者を配置するには、IoT FND でワーク オーダーを作成します。フィールド技術者は、IoT-DM クライアントを使用して IoT FND に接続し、ワーク オーダーをダウンロードします。

(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。

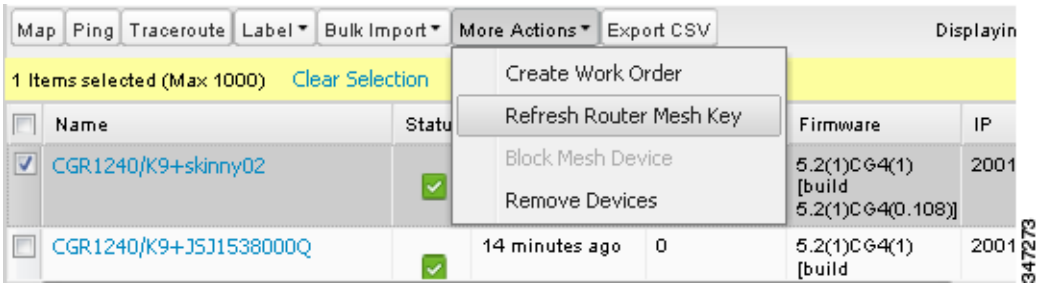
ルータ メッシュ キーの更新

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。

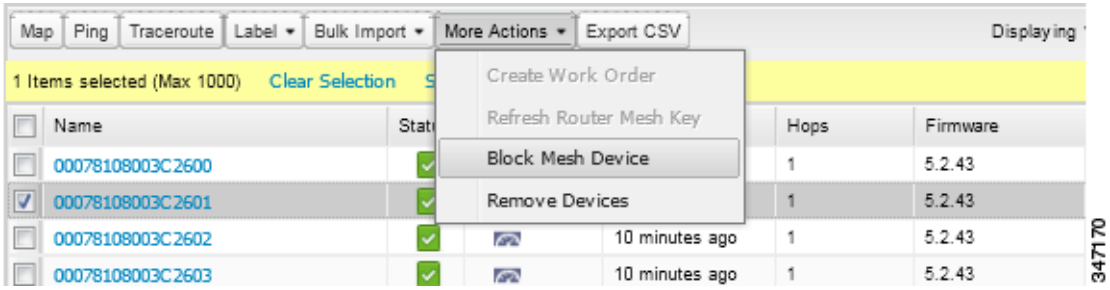
メッシュ デバイスのブロッキング

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

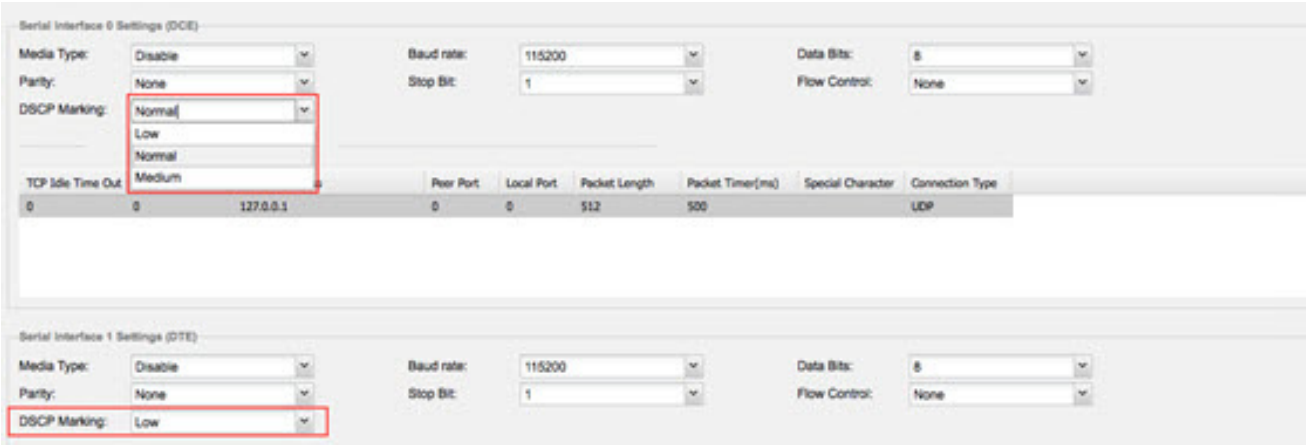
IR509 で DSCP を設定するには次の手順を実行します。

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：

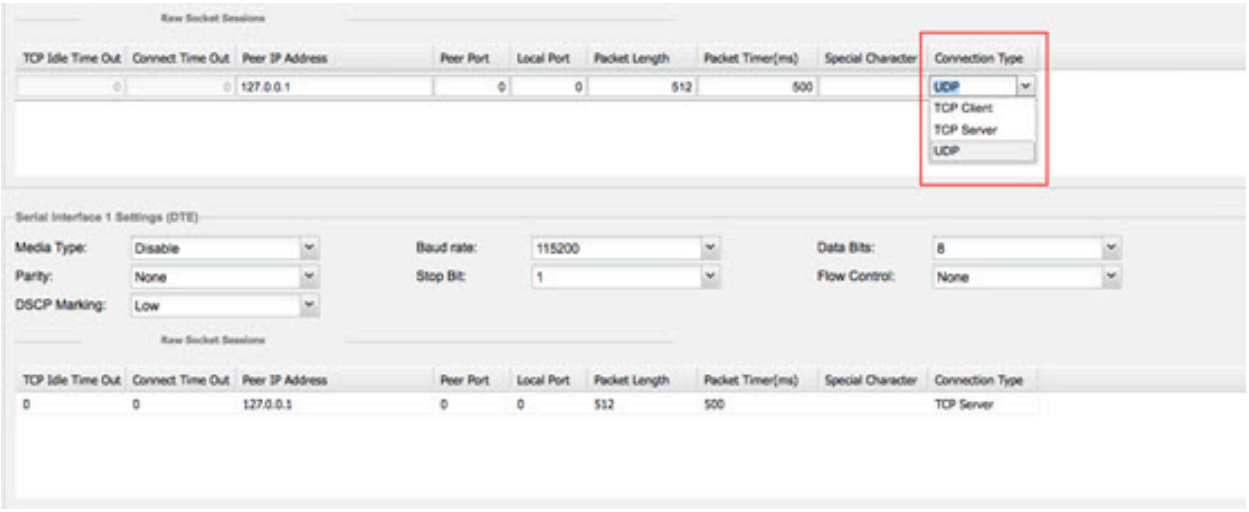
- すべてのインターフェイス（イーサネット、DTE、および DCE）で DSCP（QoS）マーキングを設定してください。オプション：Low Priority (0)、Normal Priority (10)、Medium Priority (18)。
- DSCP はインターフェイスで適用されます。DCE および DTE のデフォルト値は、Low Priority (0) です。イーサネットにはデフォルト値はありません。[Configuration Template] の値を設定していない場合、トラフィックはマーキングされていない状態でフローします。
- DCE および DTE インターフェイ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

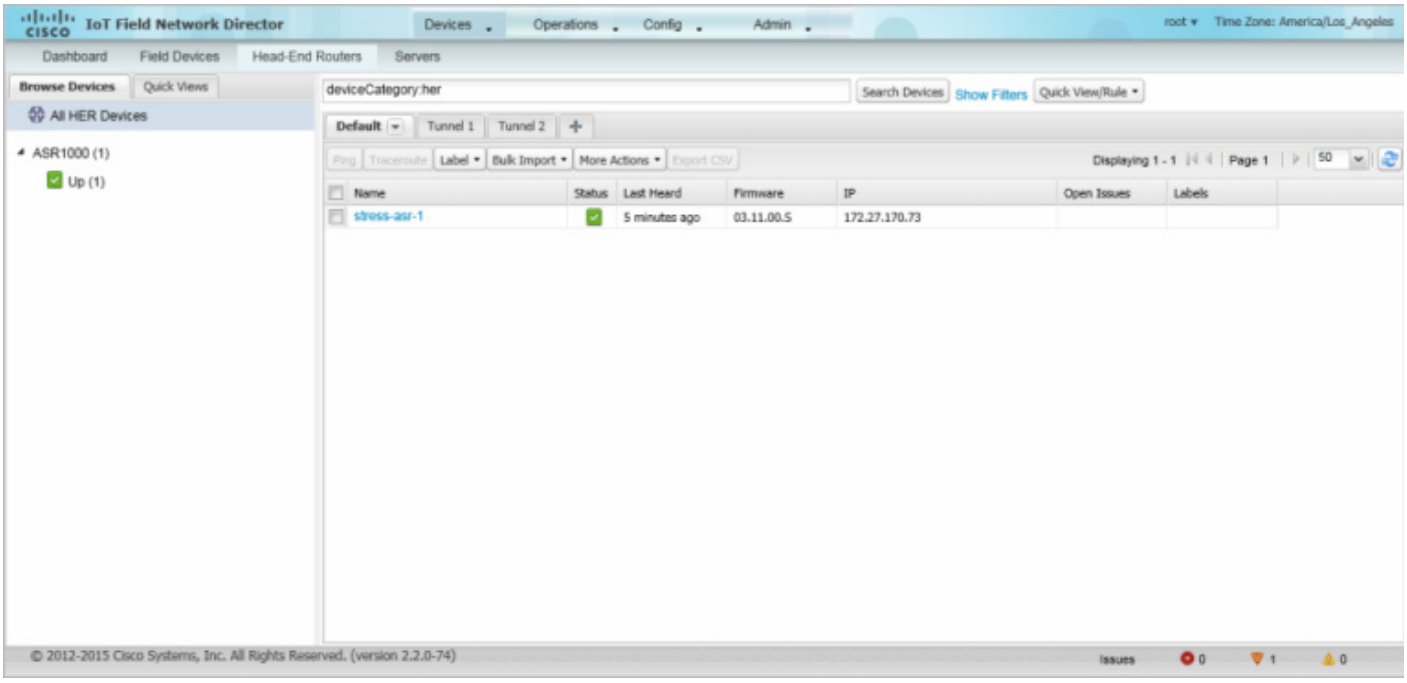
ヘッドエンド ルータの管理

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



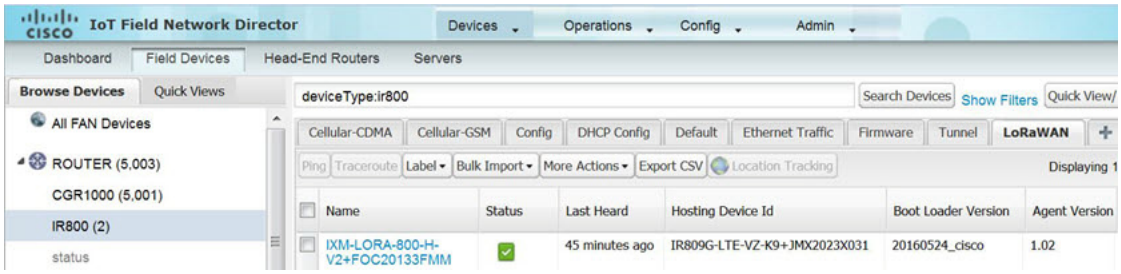
HER のビューをカスタマイズする方法については、「デバイス ビューのカスタマイズ」を参照してください。

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。



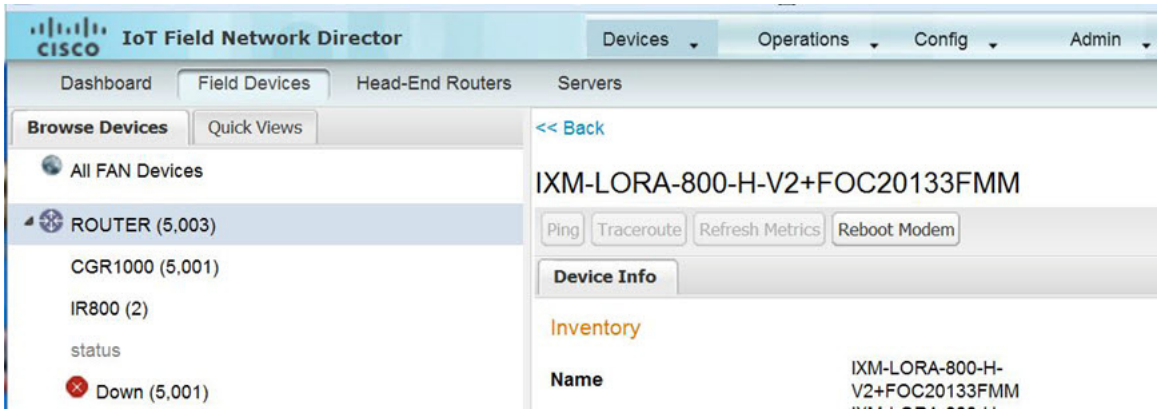
- LoRaWAN

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。



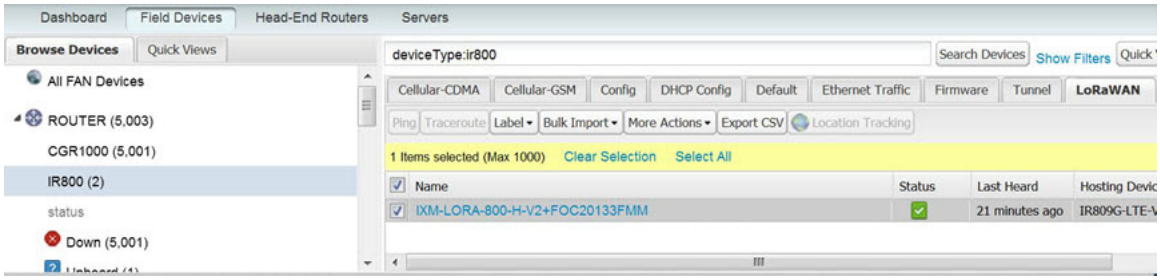
  b. [Reboot Modem] をクリックします。再起動が完了すると、LoRaWAN モジュールの [Device Info] ペインの [Last Reboot Time] フィールドに日付と時刻が表示されます。一度に処理できるモデムの再起動は 1 つだけです。

  [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

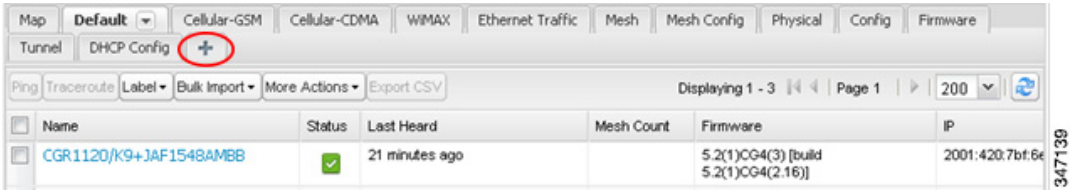
IoT FND では、デバイス ビューをカスタマイズできます。[List] ビューでは、次の操作を実行できます。

- 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

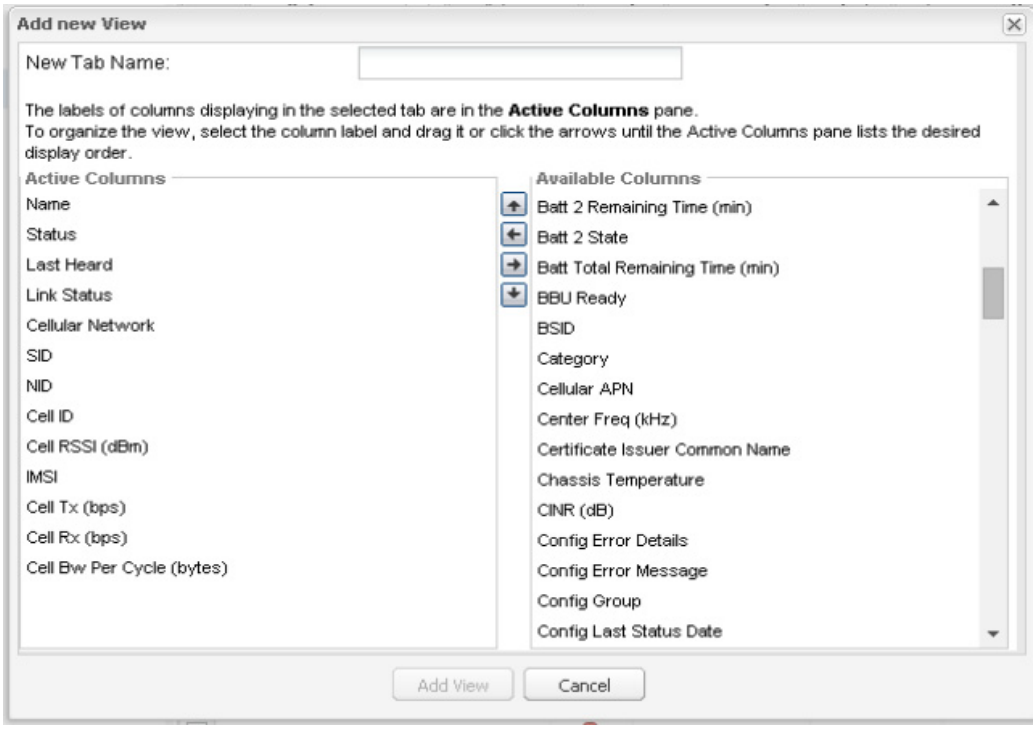
デバイス ビューの追加

[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

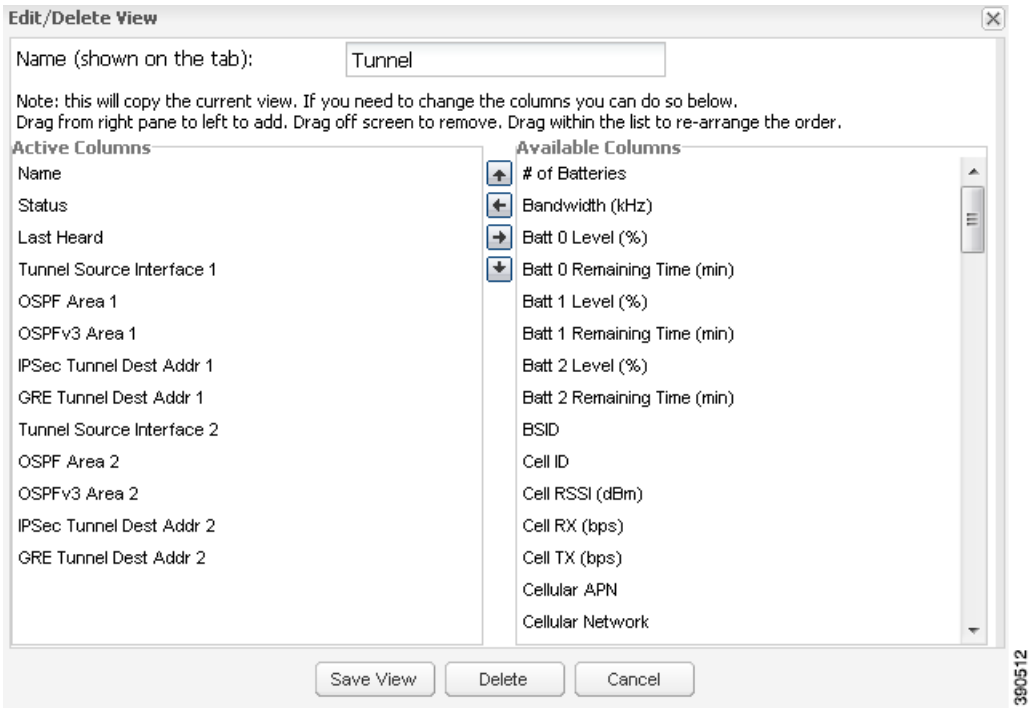
デバイス ビューを編集するには、次の手順を実行します。

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。

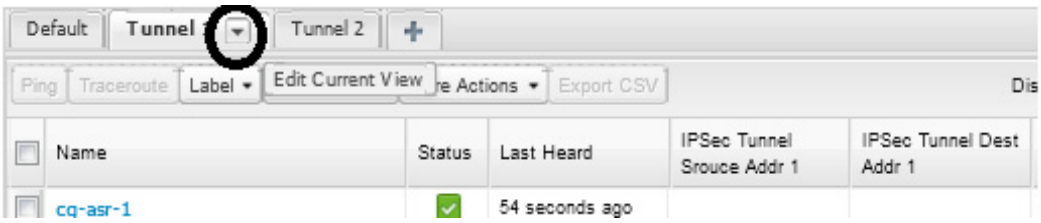


3. [Save View] をクリックします。

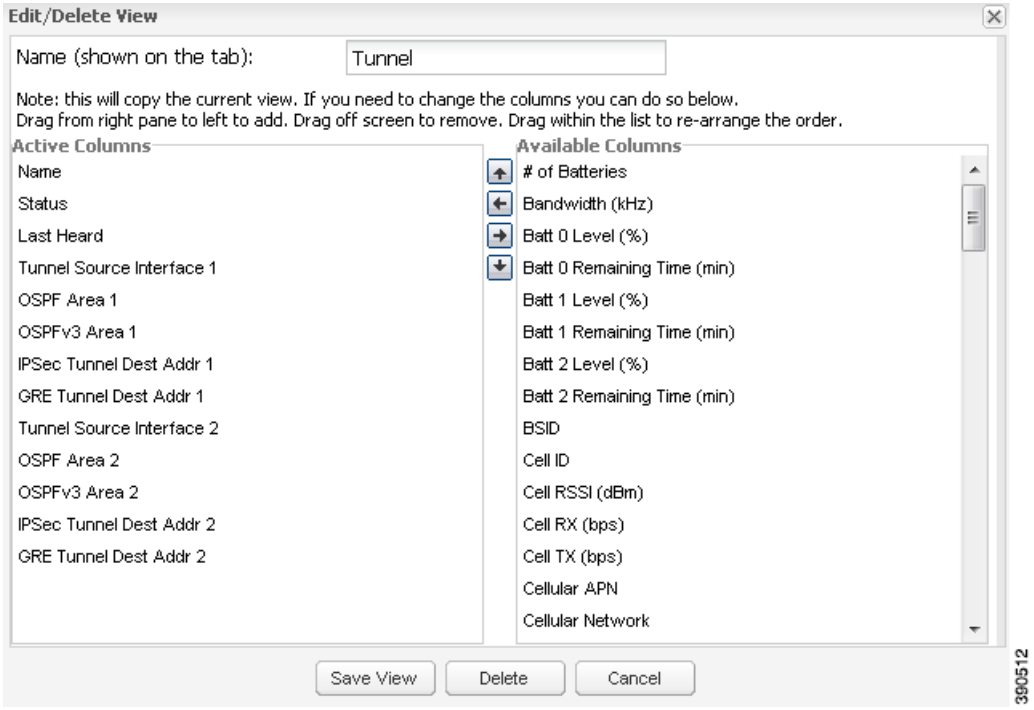
デバイス ビューの削除

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。



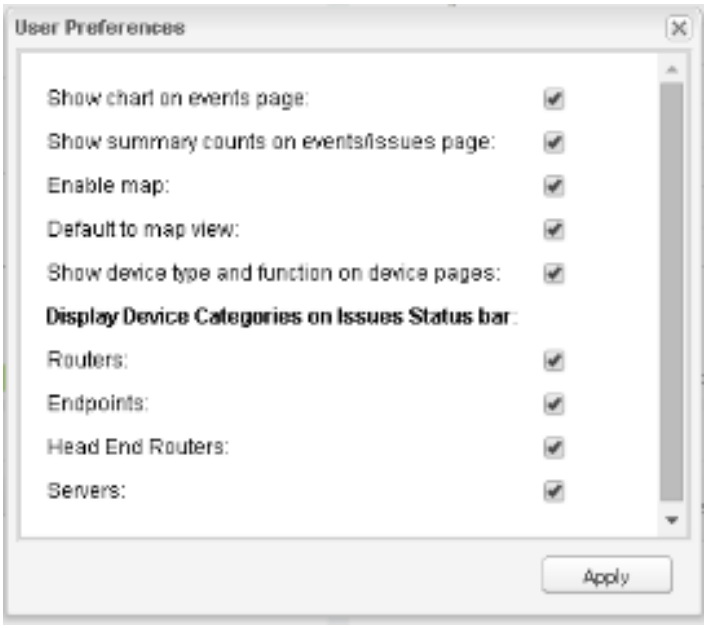
3. [Delete] をクリックします。

[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。

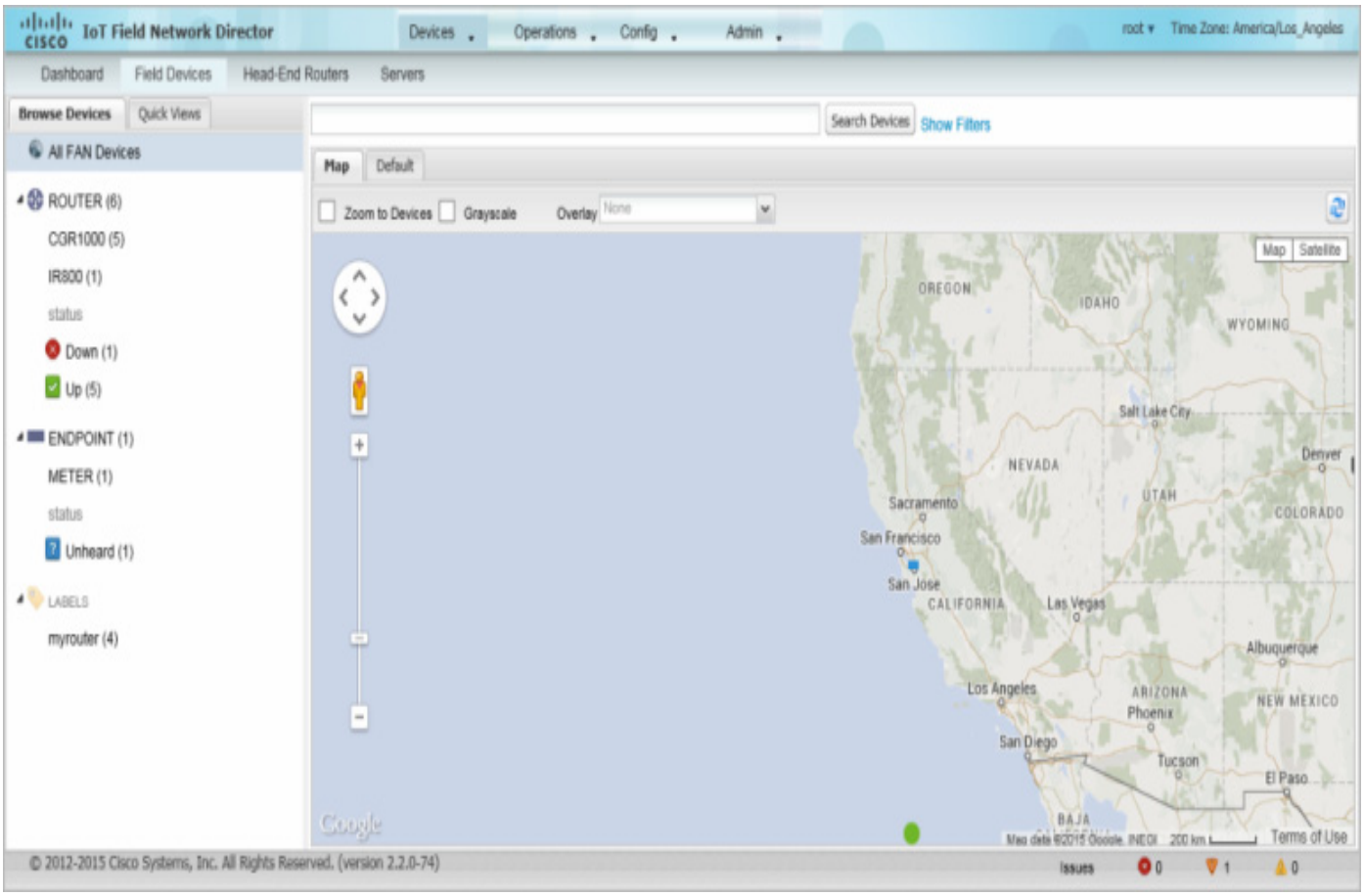
[Map] ビューにデバイスを表示するには、次の手順を実行します。

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。

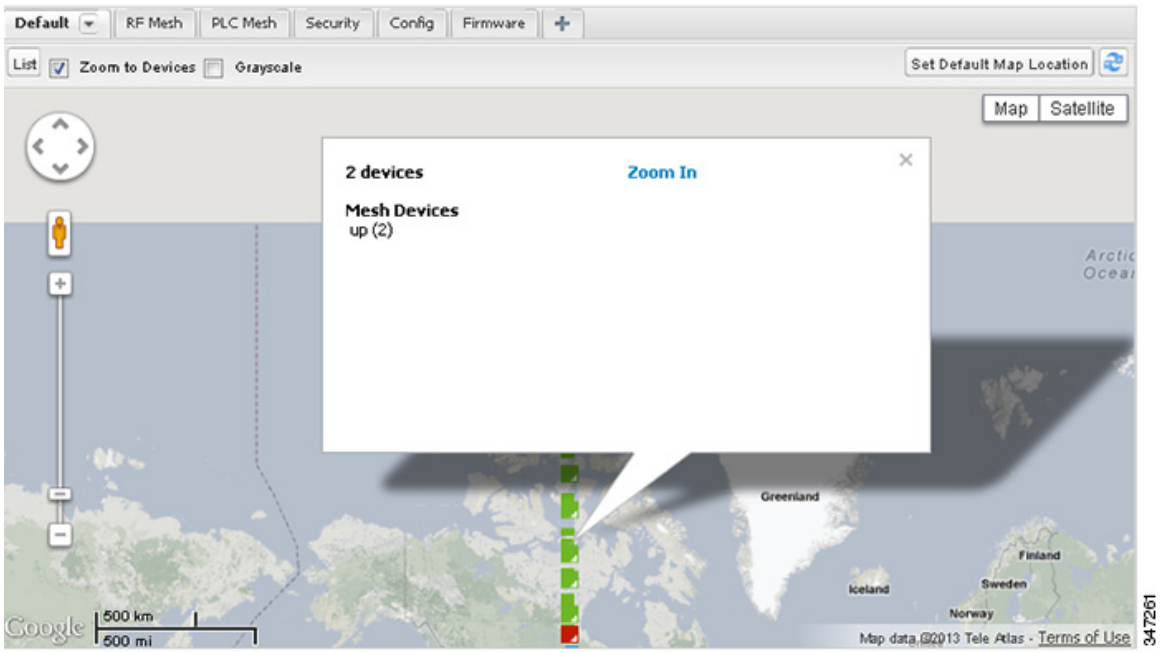


2. [Devices] > [Field Devices] を選択します。
3. [Map] タブをクリックします。

   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。



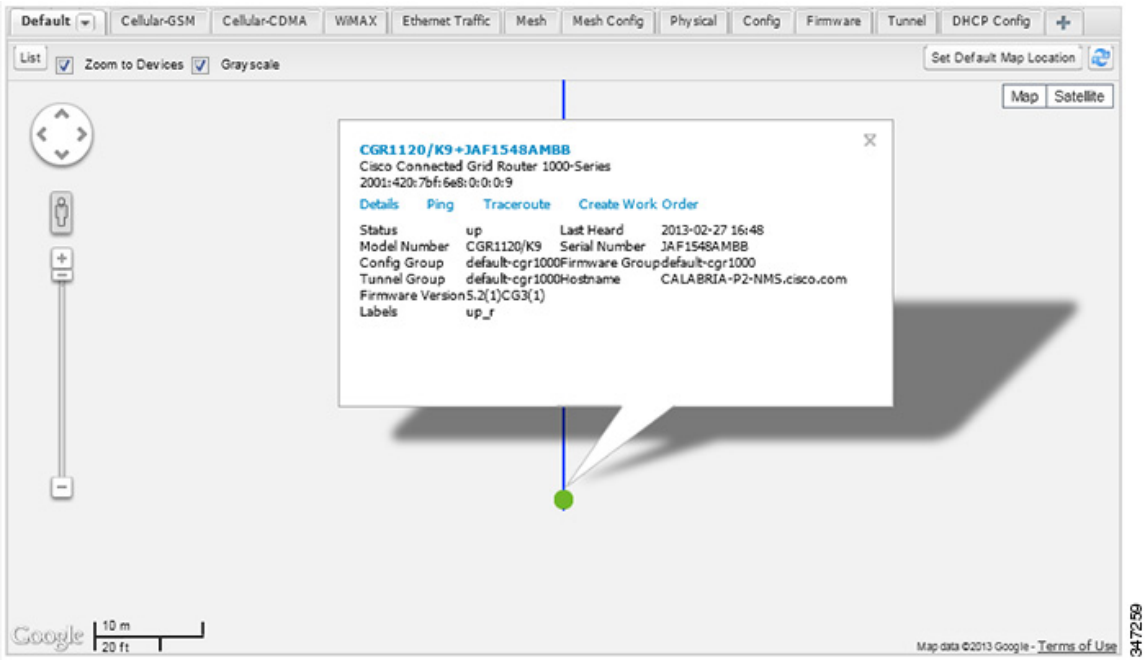
個々のデバイスを確認するには、デバイス アイコンが見えるまでズーム インします。また、デバイスをクリックして [Zoom In] リンクを含むポップアップ ウィンドウを表示し、マップ表示をデバイス レベルに移動することもできます。



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。

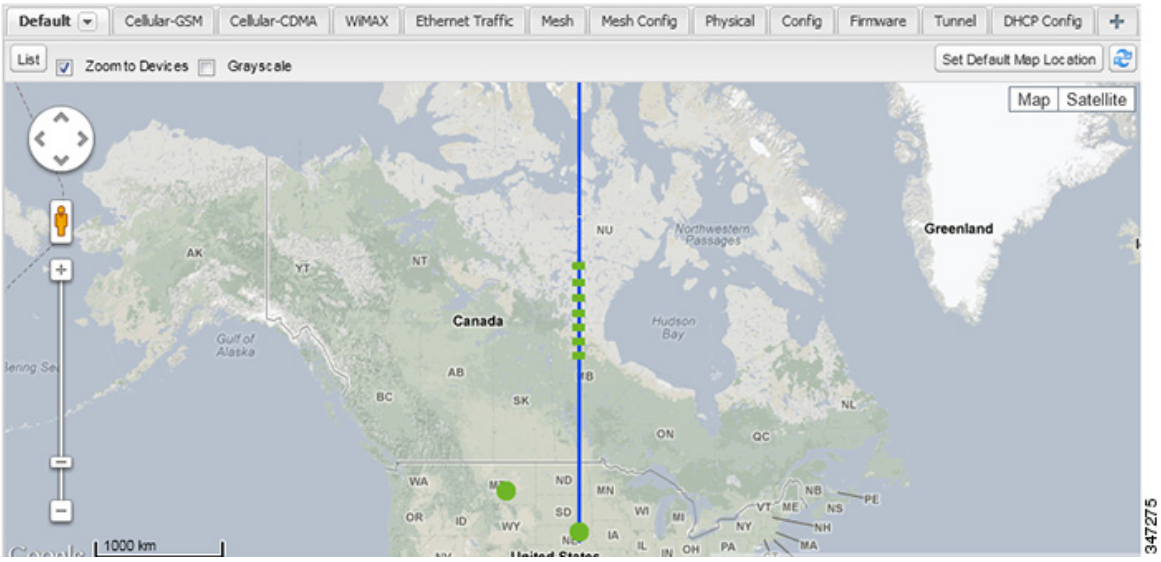


デバイスまたはグループの基本的な情報がリスト表示されたポップアップ ウィンドウが表示されます。

- 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。

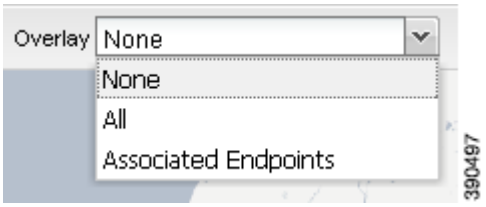
マップの設定

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。

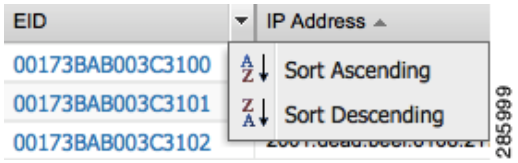
1. [Devices] > [Field Devices] を選択します。
2. [Map] タブをクリックします。
   - デバイスを自動ズームするには、[Zoom to Devices] チェックボックスをオンにします。
   - マップをグレースケール表示するには、[Grayscale] チェックボックスをオンにします。
   - すべての関連付けられているワイヤレス パーソナル エリア ネットワーク（WPAN）をマップ上にオーバーレイするには、[Overlay] ドロップダウン メニューから [Associated WPAN Endpoints] を選択します。



   - 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

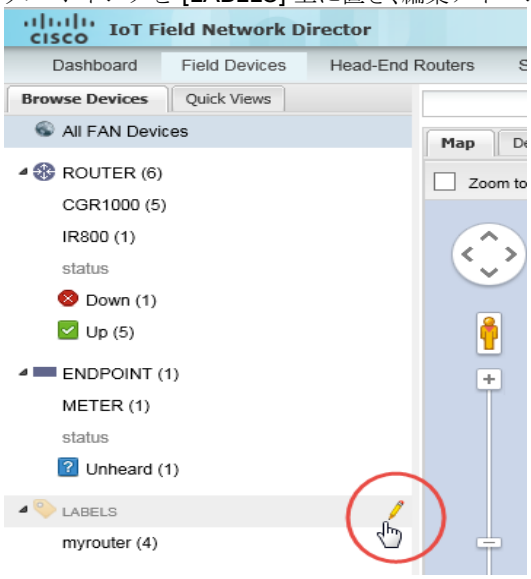
デバイスの配置およびデバイスの管理を容易にするには、ラベルを使用してデバイスの論理グループを作成します。

ラベルの管理

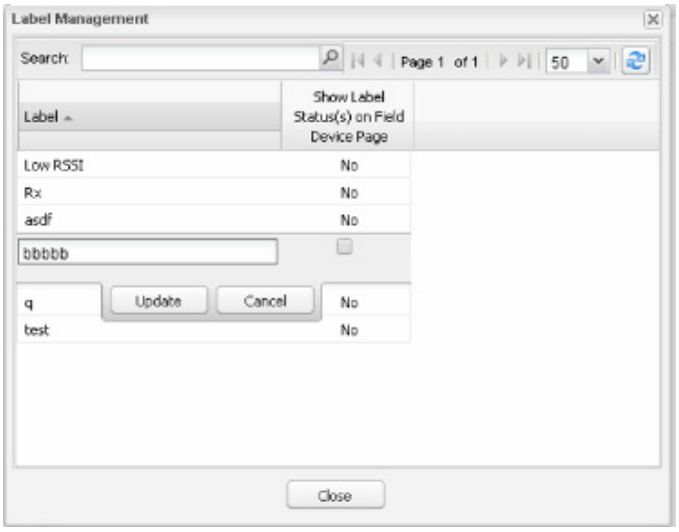
[Label Management] ウィンドウを使用して、すべてのカスタム ラベル、ラベル プロパティ、およびカスタム ラベルの検索を表示します。

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。

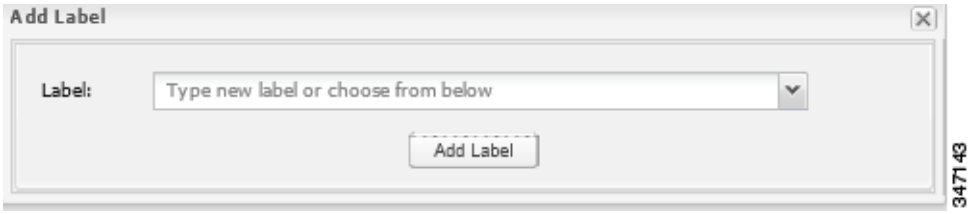
- ラベル プロパティを変更するには、ラベル行をダブルクリックし、ラベル名およびデバイス ステータスの表示設定を編集します。

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。

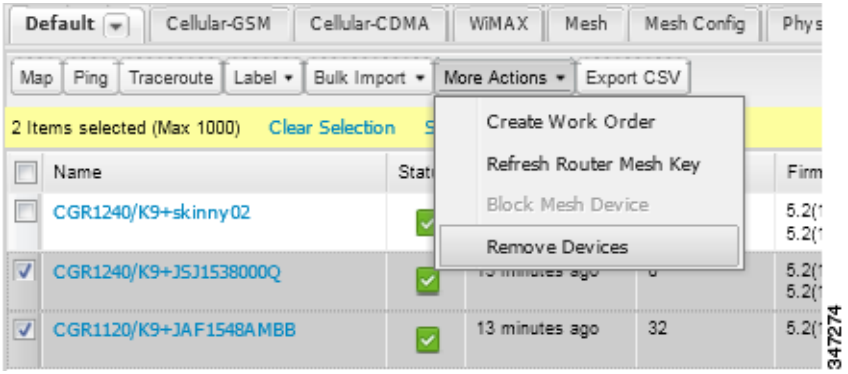
ラベルを一括して削除する場合は、「ラベルの一括削除」を参照してください。

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。

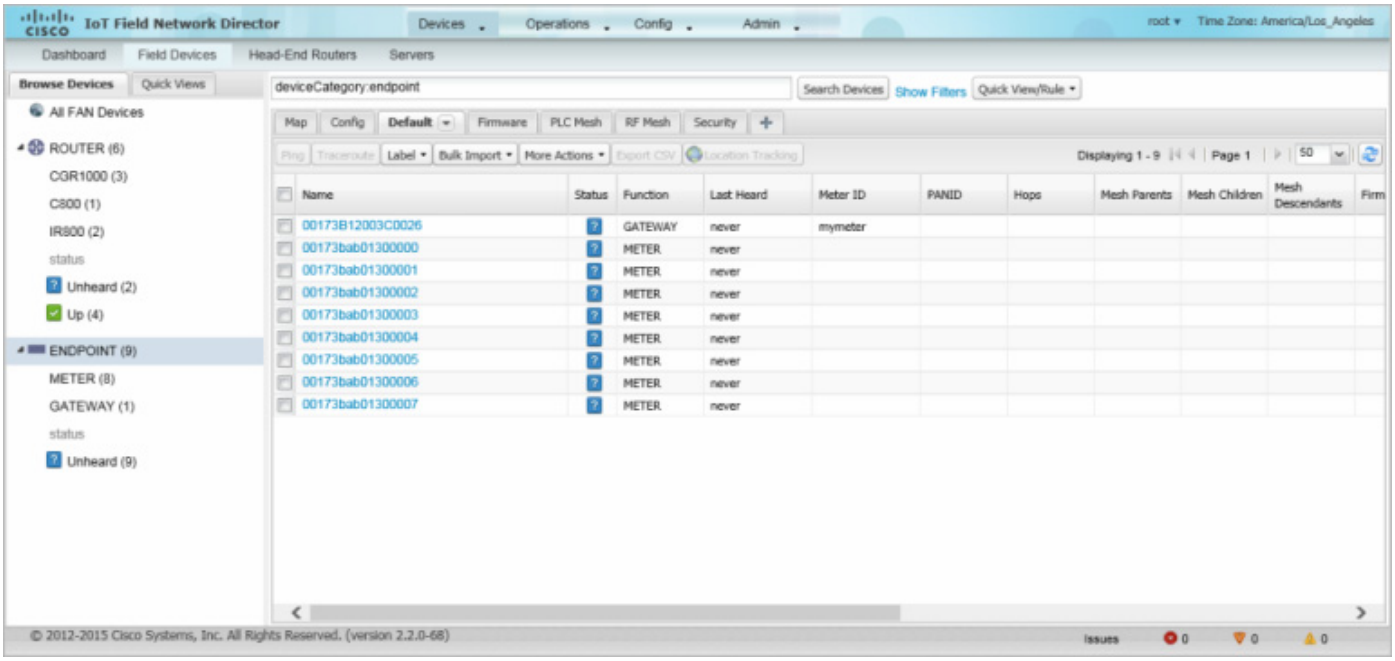
フィルタを使用したデバイス表示の制御

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。

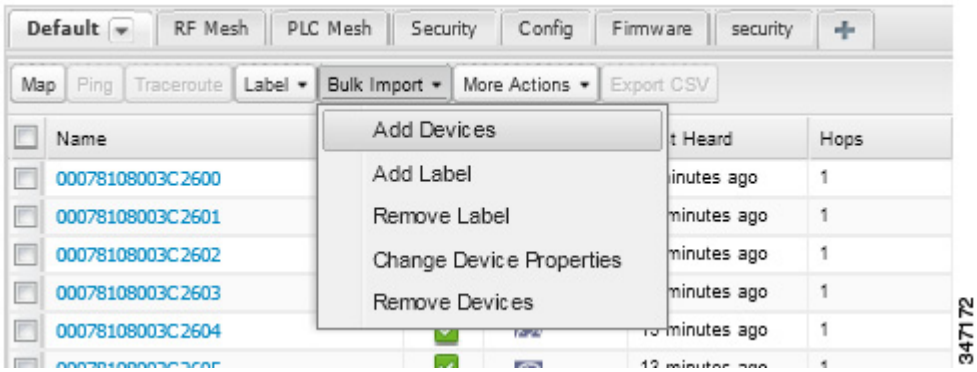
- デバイスの一括追加
- デバイスの一括削除
- デバイス プロパティの一括変更
- ラベルの一括追加
- ラベルの一括削除

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
```

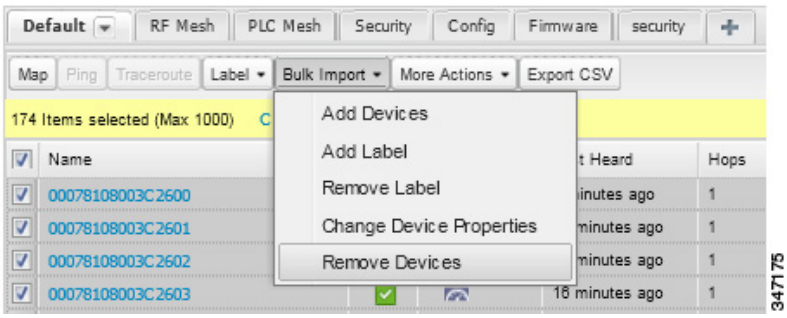
デバイスの一括削除

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。

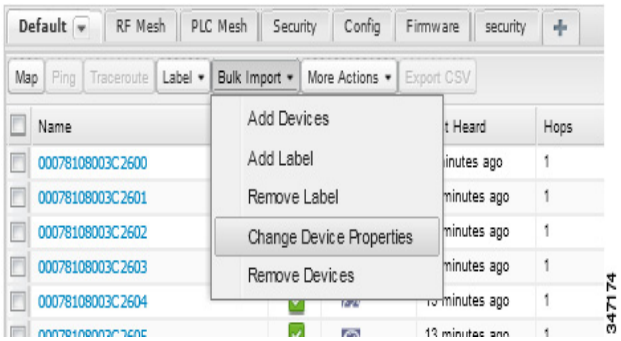
デバイス プロパティの一括変更

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。

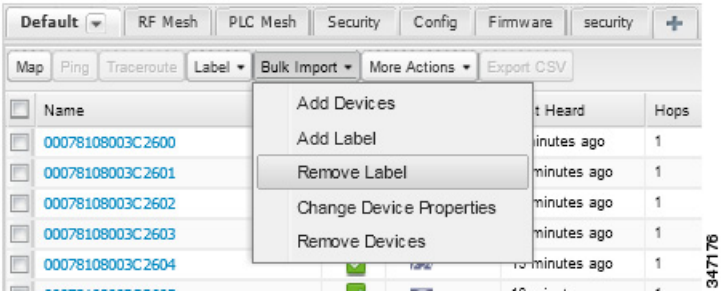
5. 終了したら、[Close] をクリックします。

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。

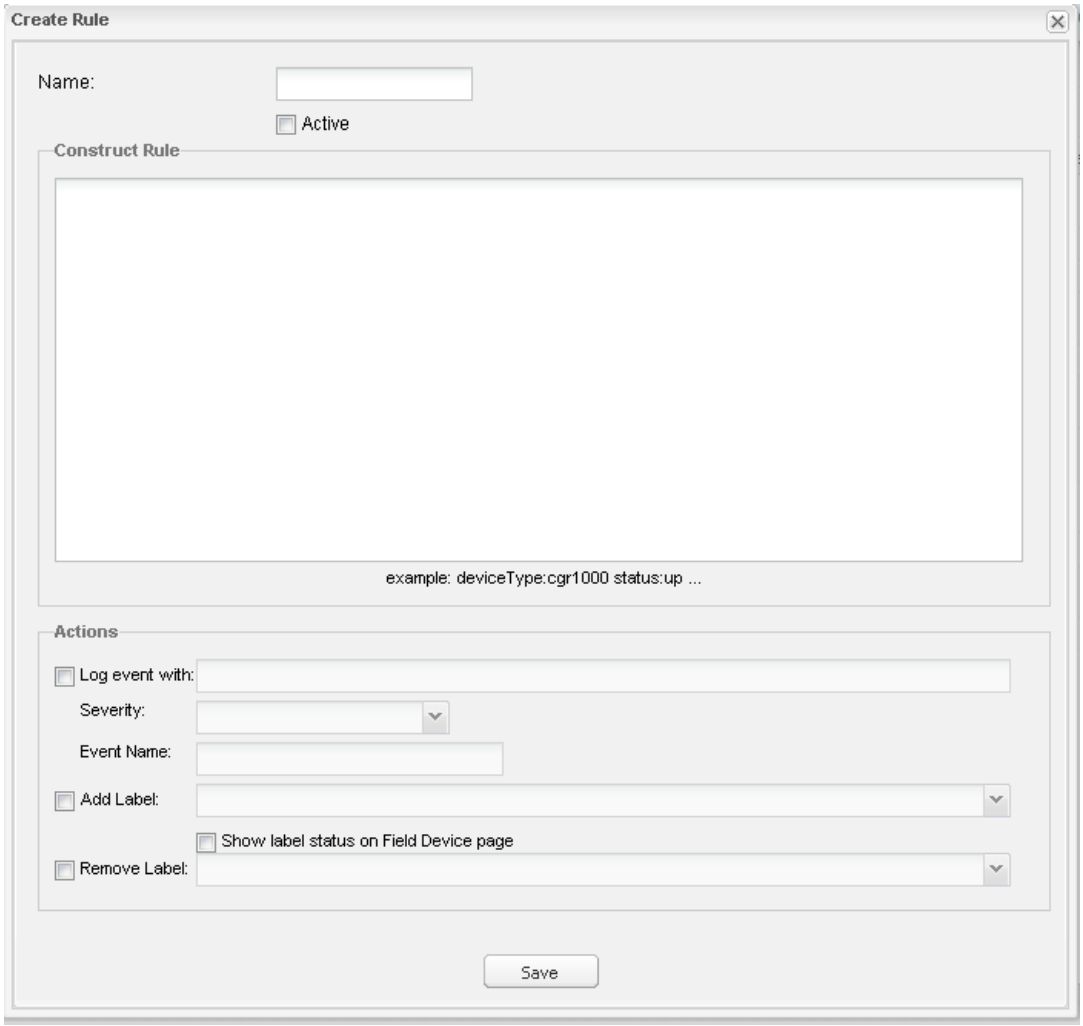
   ルールの編集方法の詳細については、「ルールの追加」を参照してください。

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

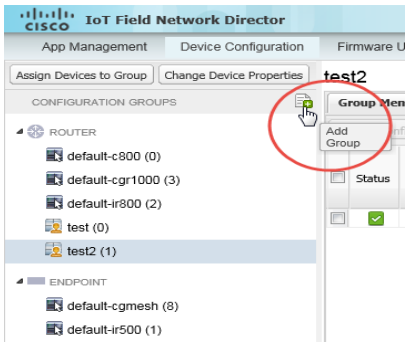
ROUTER グループの作成

(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。

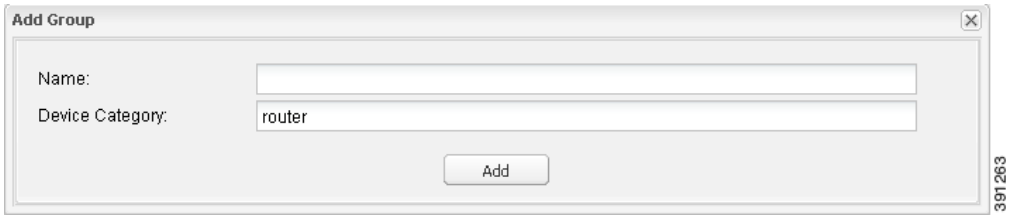
ROUTER 設定グループを作成するには、次の手順を実行します。

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。

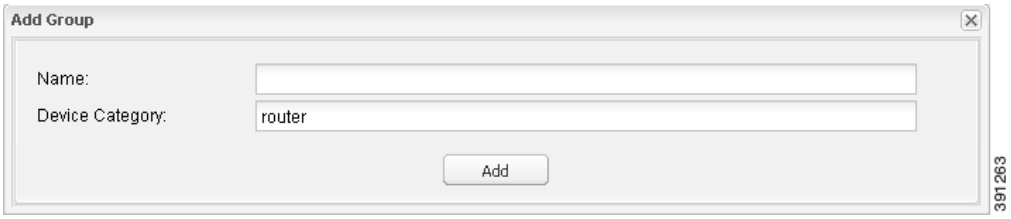
[ROUTERS] リスト(左ペイン)に新しいグループ エントリが表示されます。

- 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。

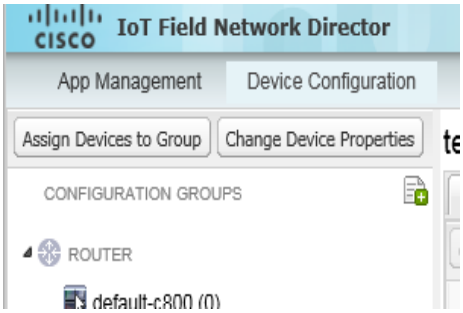
- グループの名前を変更する場合は、「デバイス設定グループの名前変更」を参照してください。
- グループを削除するには、「デバイス グループの削除」を参照してください。

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

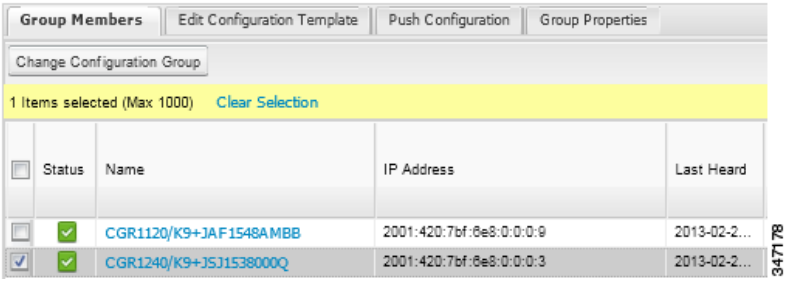
デバイスをグループ間で移動するには、次の 2 つの方法があります.

- 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

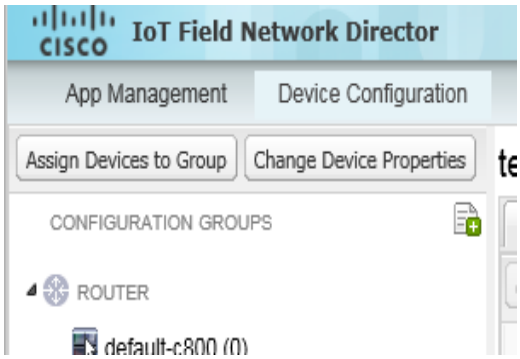
多数のデバイスをグループ間で移動する場合は、移動するデバイスのリストを含む CSV ファイルをインポートします。

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。

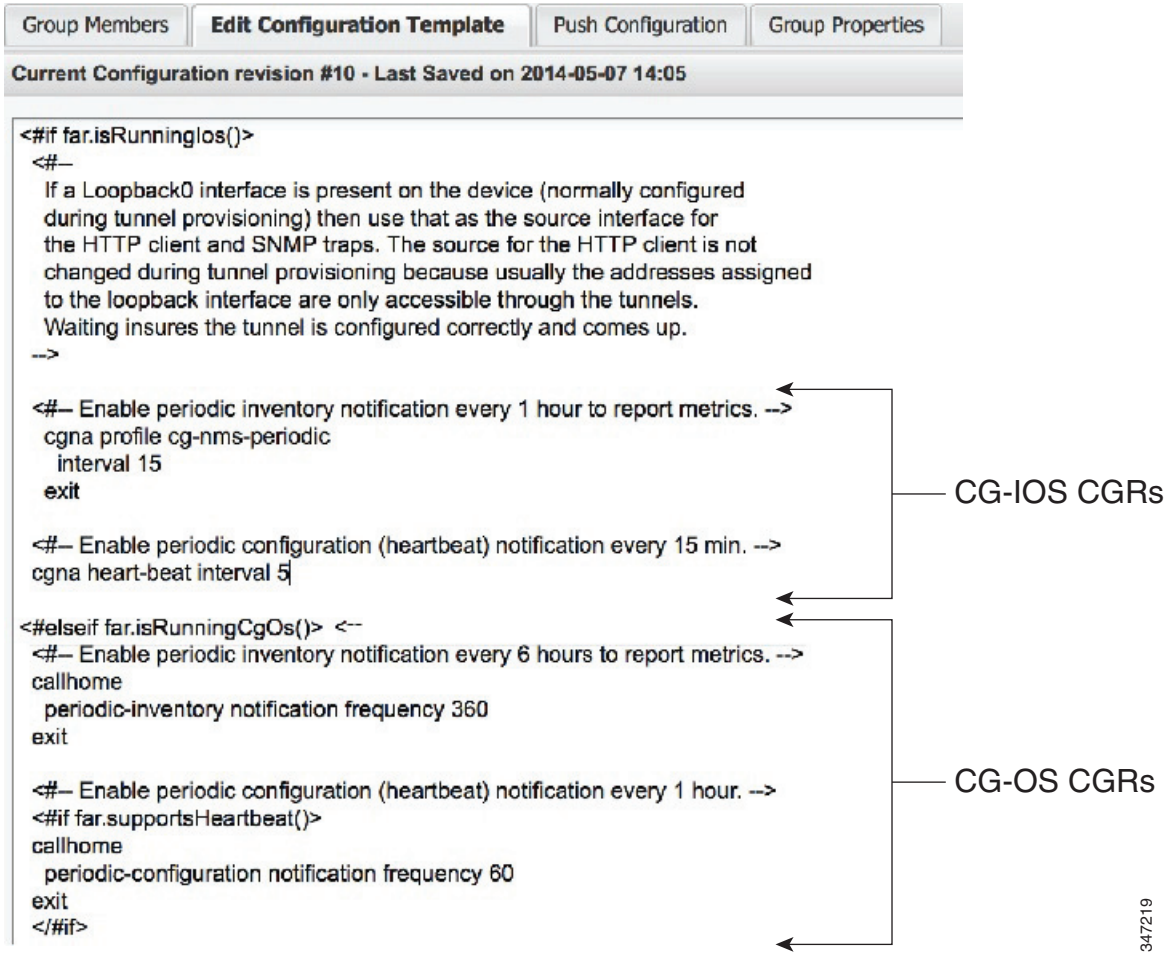
グループの [Group Properties] タブをクリックし、[Mark Routers Down After] フィールドの値を変更することにより、マーク ダウン タイマーを設定できます。

- 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
     ```

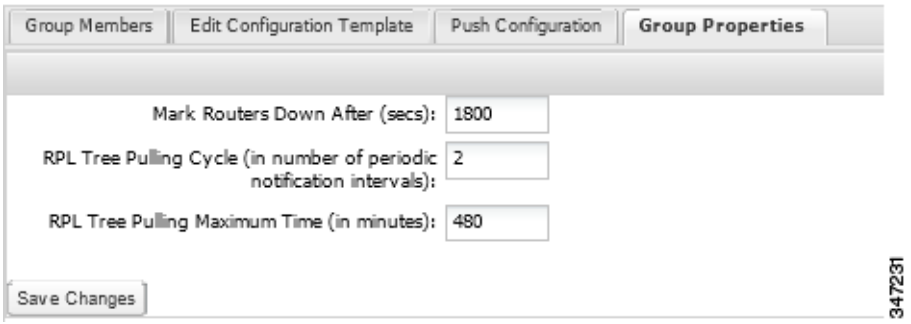
   - CG-OS CGR の場合は、**periodic-inventory notification frequency** のパラメータ値を新しい値に変更します。時間の値は分単位です。

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

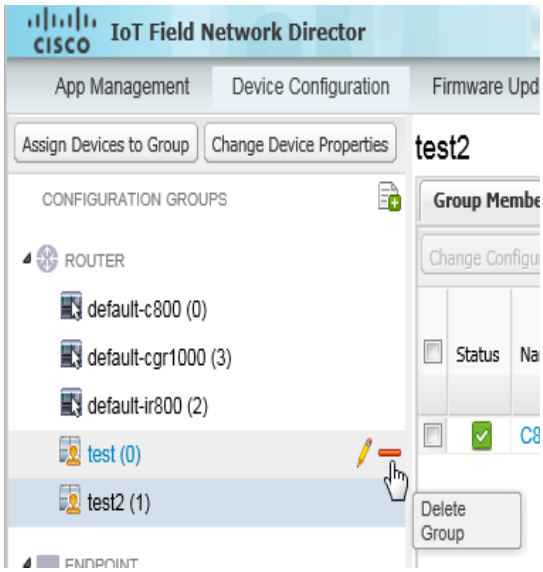
デバイス設定グループの名前を変更するには、次の手順を実行します。

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。

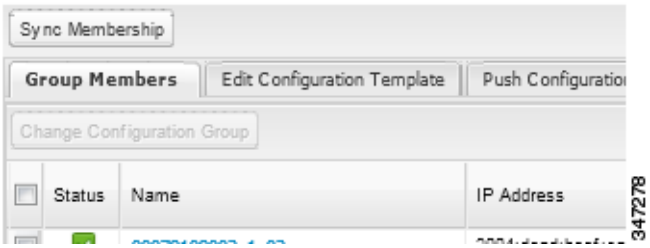
エンドポイント メンバーシップの同期

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。

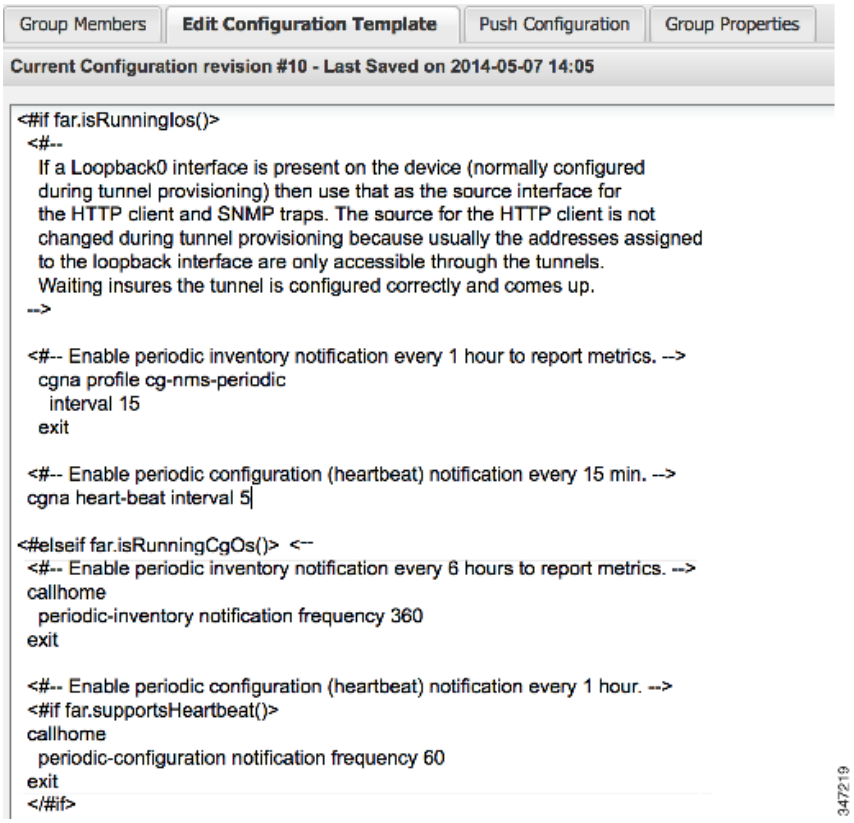
デバイスが最初に同期されるのは、IoT FND に登録した後です。

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。

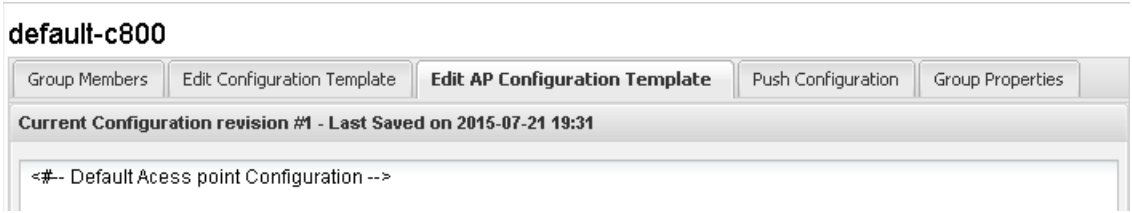
IoT FND は変更内容をデータベースにコミットし、テンプレートのバージョン番号を増やします。

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

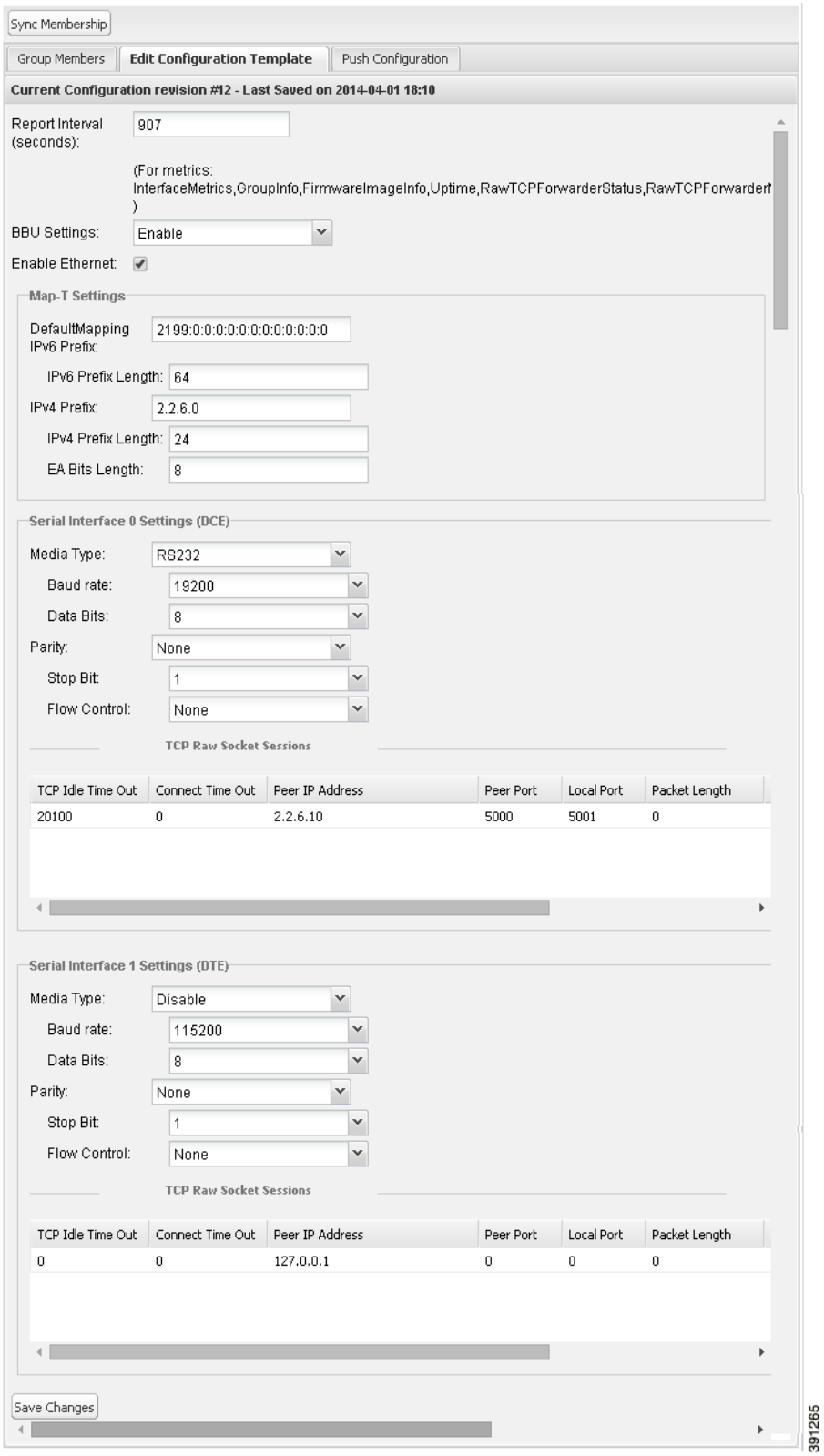
Cisco IOS ルータで、SNMP v3 情報イベントを設定して、デフォルトの SNMP v3 トラップを置き換えます。CG-OS ではデフォルトで、ルータ上にトラップを生成する IoT FND イベント関連の変更に対して SNMP v3 トラップが設定されます。IoT FND は、これらのトラップを対応するイベントにマッピングします。Cisco IOS ルータでは、これらの SNMP v3 トラップを SNMP v3 情報イベントに変換することにより、ルータからイベントを受信するたびにルータに確認が送信されます。これにより、ルータはトラップが IoT FND により受信されたことを確認します。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。

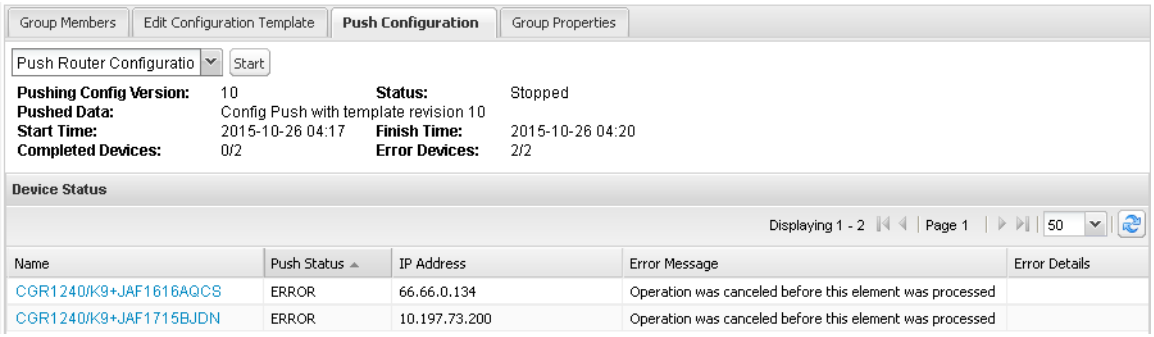
IoT FND は変更内容をデータベースにコミットし、バージョン番号を増やします。

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

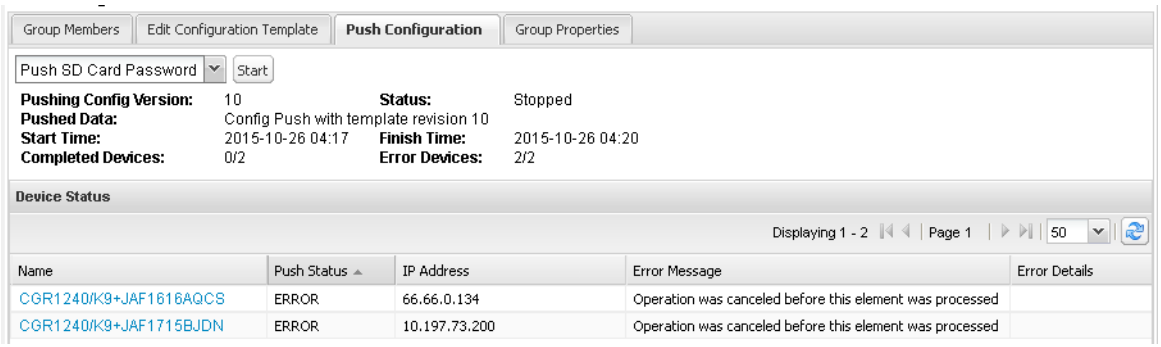
CGR SD カードのパスワード保護により、不正アクセスを防止し、CGR SD カードを他のパスワードで他のシステムに転用することを防ぐことができます。

（注）これは、C800 および IR800 には適用されません。

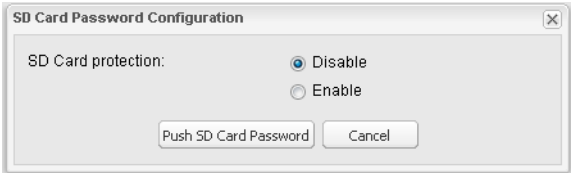
[Device Info] ペインの [Inventory] セクションに、CGR SD カードのパスワード保護のステータスが表示されます。[Config Properties] タブの [Router Credentials] セクションには、SD カードのパスワードが表示されます。

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

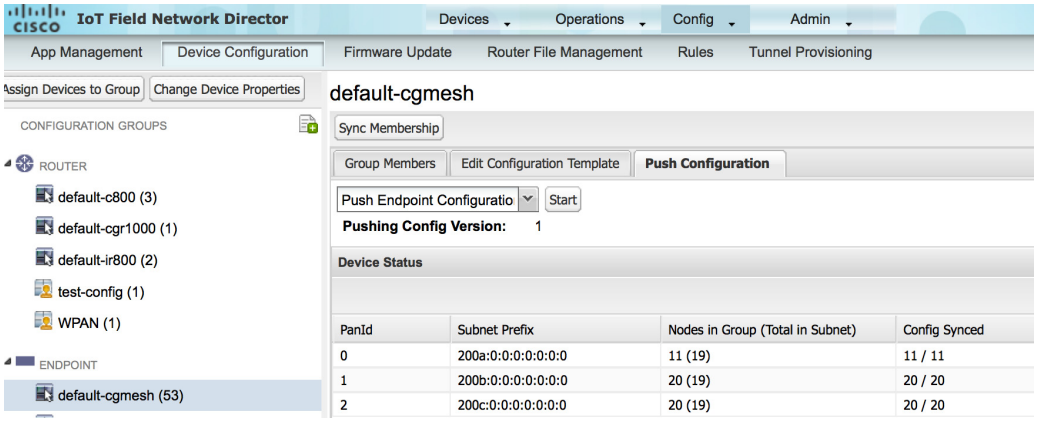
メッシュ エンドポイントに設定をプッシュするには、次の手順を実行します。

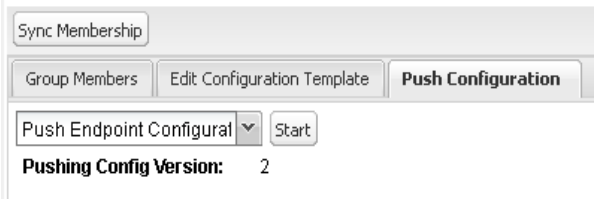
1. [Config] > [Device Configuration] を選択します。
2. グループまたはグループのサブセットを選択し、設定を [ENDPOINT] リストにプッシュします。

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

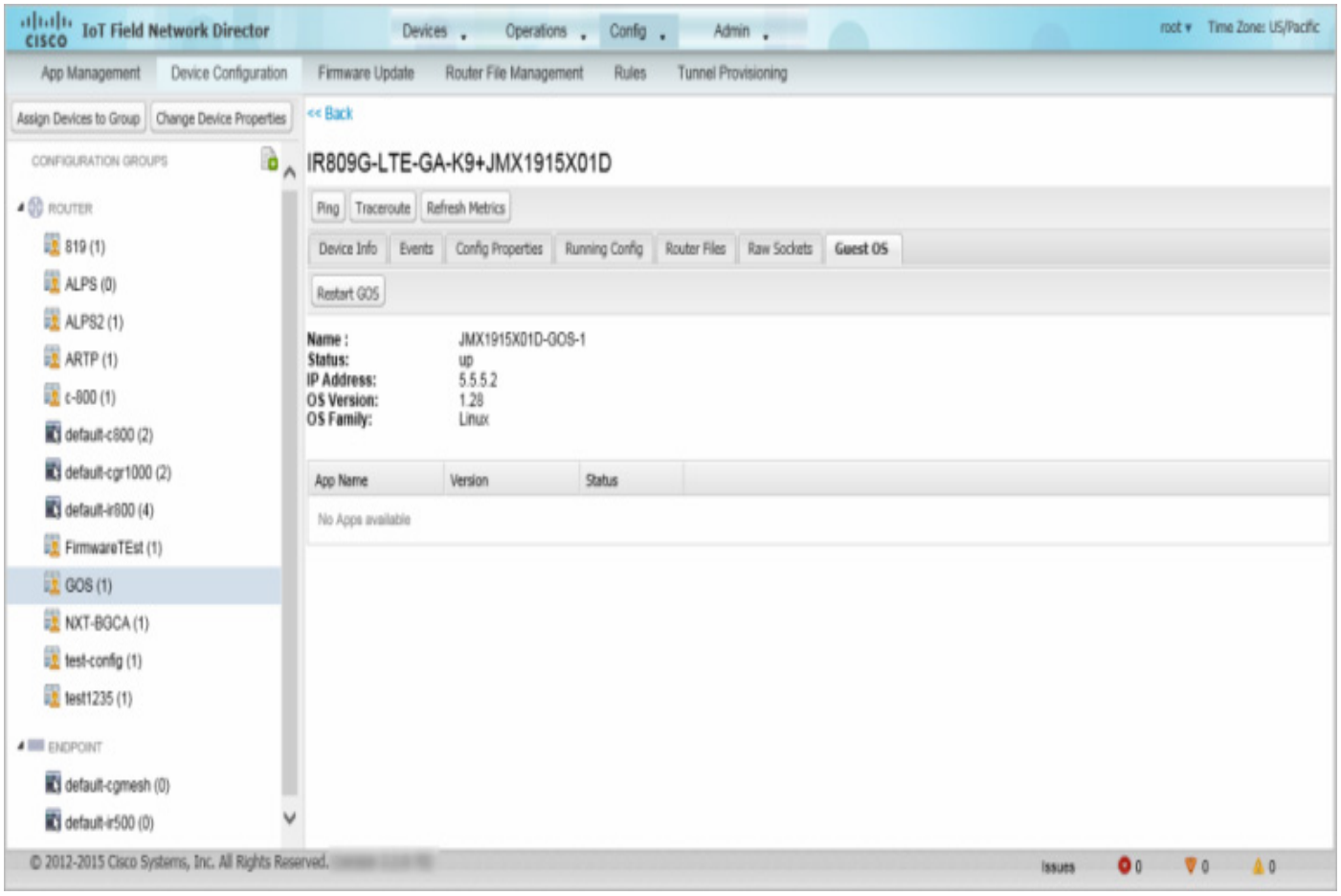
Cisco IOS CGR は仮想マシンをサポートし、Cisco IOS 仮想マシンの横で実行中のゲスト OS（GOS）インスタンスでアプリケーションを実行します。GOS は、Linux です。GOS 上で動作するアプリケーションは通常、モニタリングおよびアカウンティング目的で、フィールドから統計情報を収集します。Cisco IOS ファームウェア バンドルでは、CGR 上の VM インスタンスに参照 GOS がインストールされます。IoT FND は、GOS で、次のロールベースの機能をサポートします。

- 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。

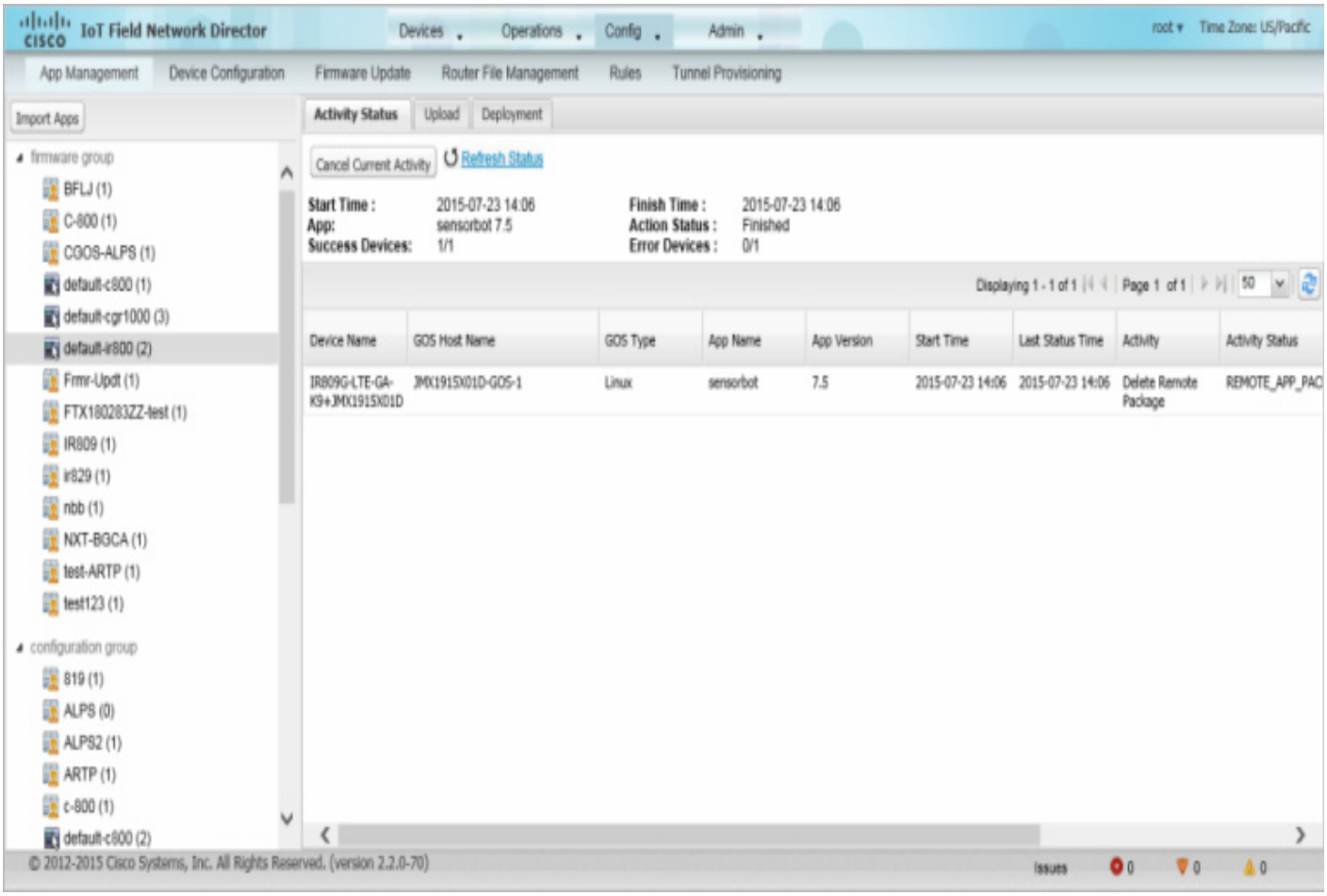
GOS アプリケーションの管理

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。

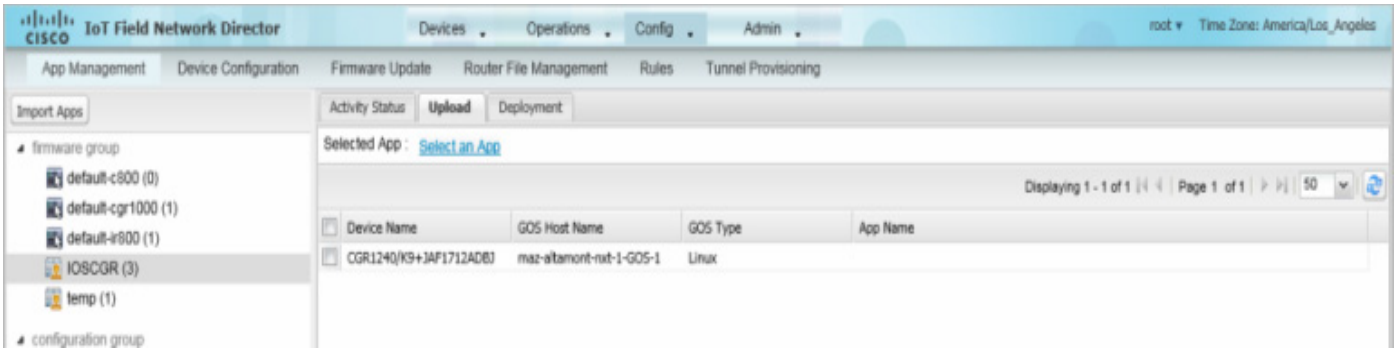
[Activity Status] タブでは、次の操作も行うことができます。

- [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。

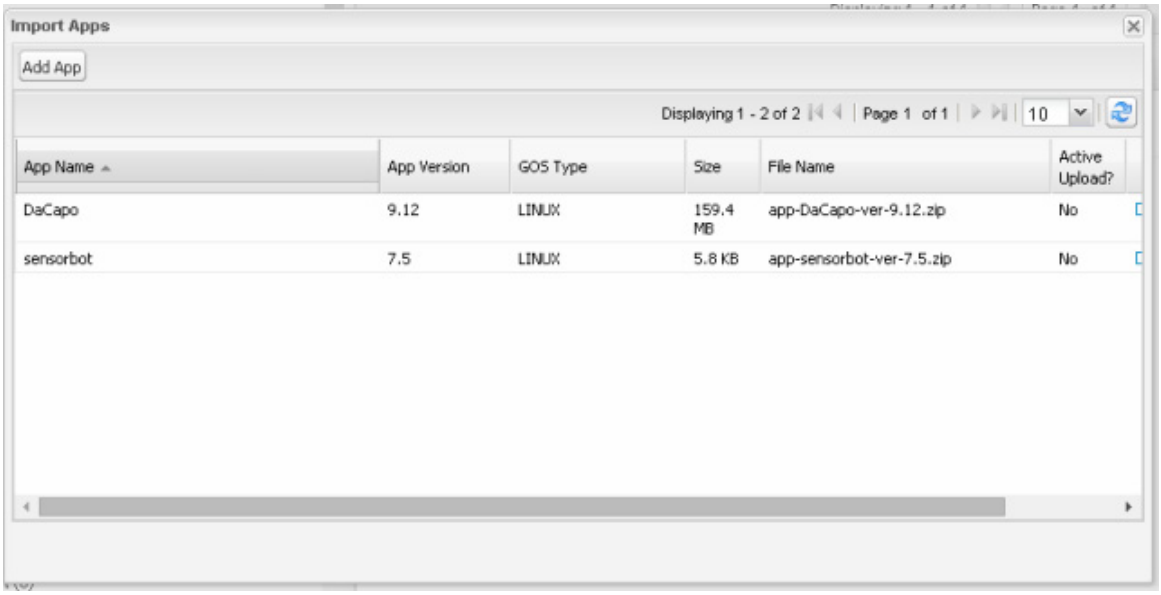
図 8　[Upload] タブ



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。

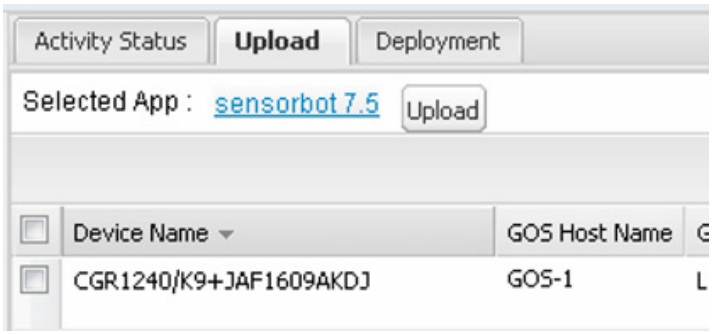
   アプリケーション ファイルは NMS サーバにアップロードされ、[App Name] リストに表示されます。

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。

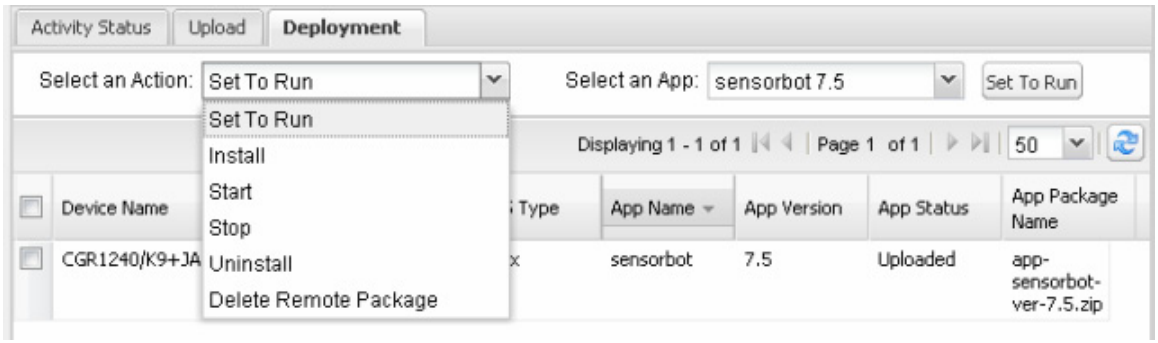
GOS アプリケーションの導入

[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。

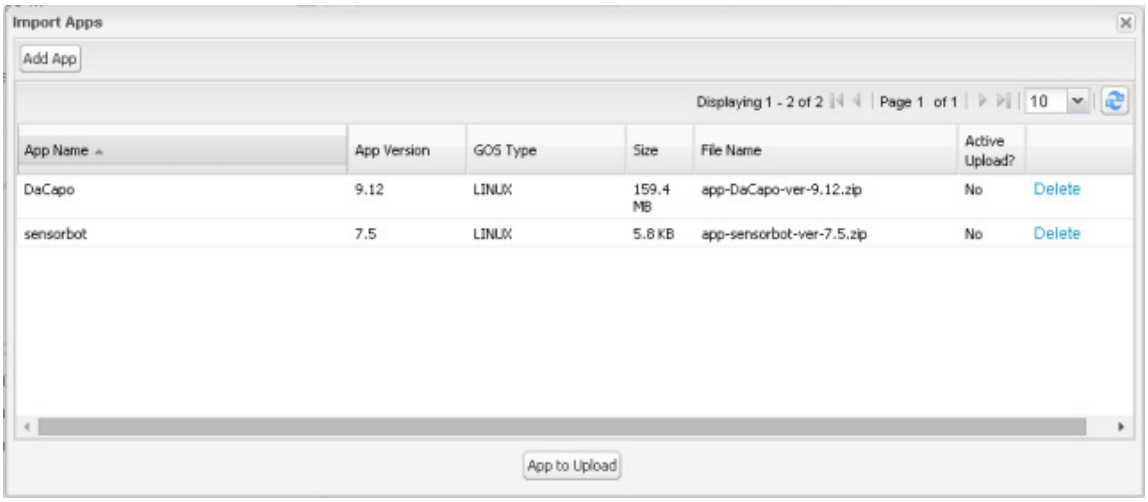
アクティビティが開始します。[Activity Status] タブでアクティビティの進行状況をモニタできます。

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。



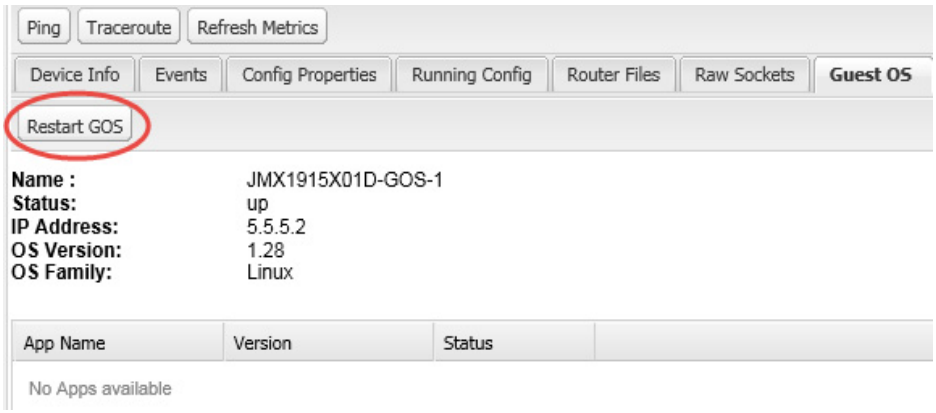
5. 確認ダイアログボックスで [OK] をクリックします。

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。

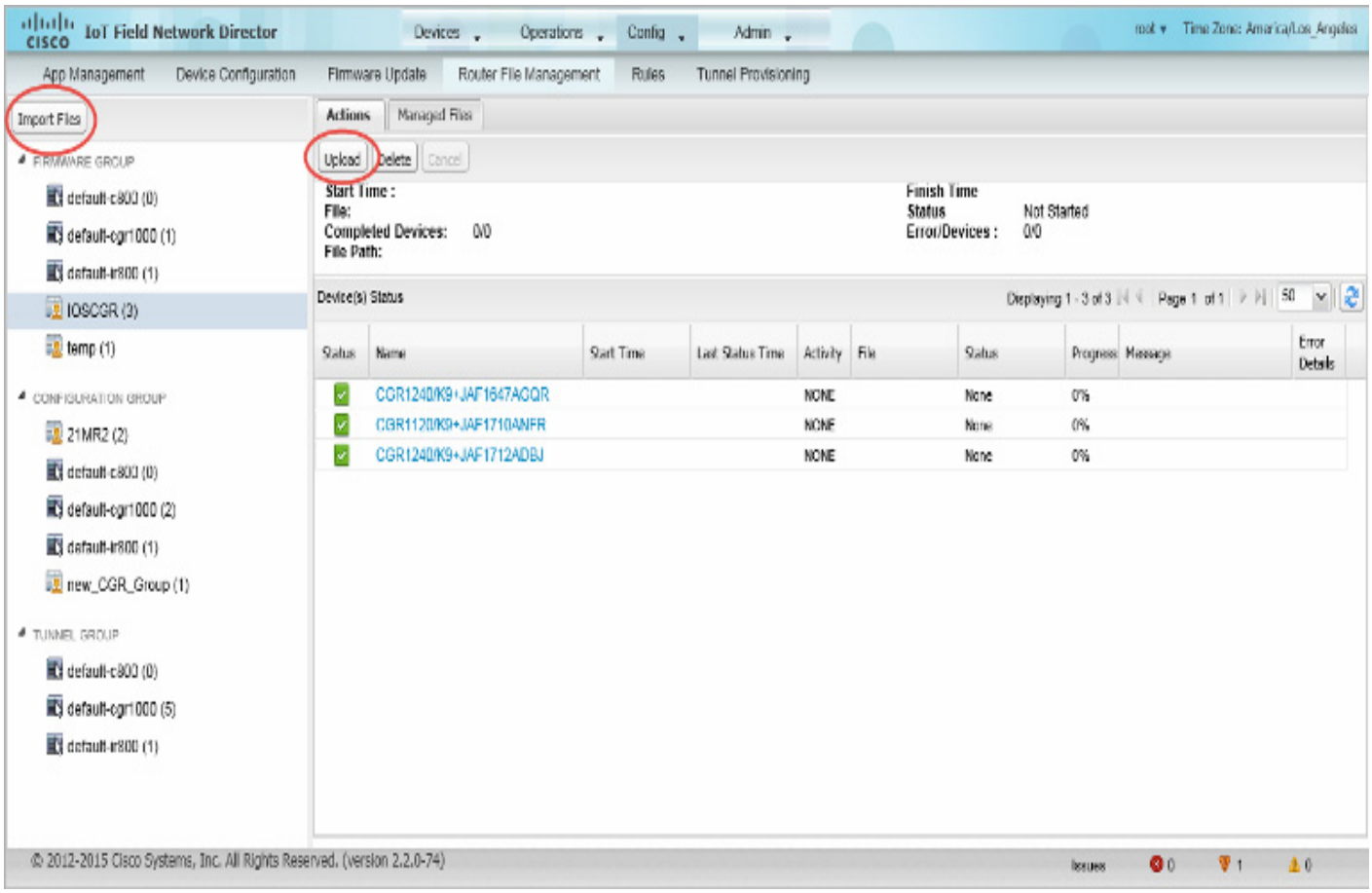
また、ファイル管理機能の向上のために、他のファイル タイプを FAR に転送することもできます。FAR にファイルをアップロードするには、最初にファイルを IoT FND にインポートする必要があります。IoT FND はファイルを処理し、次の属性を使用して IoT FND に保存します。

- 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

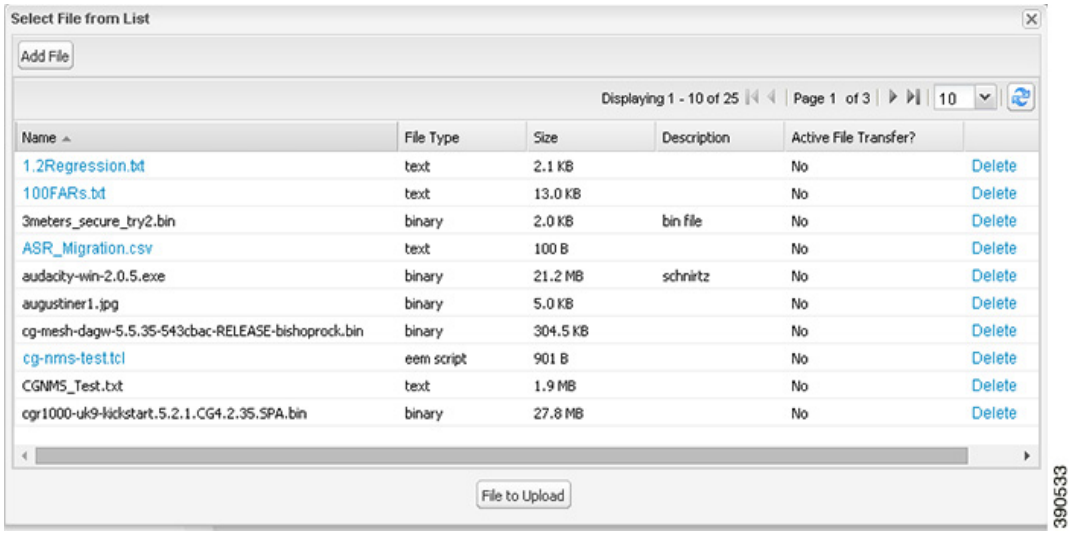
IoT FND にファイルを追加するには、次の手順を実行します。

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。



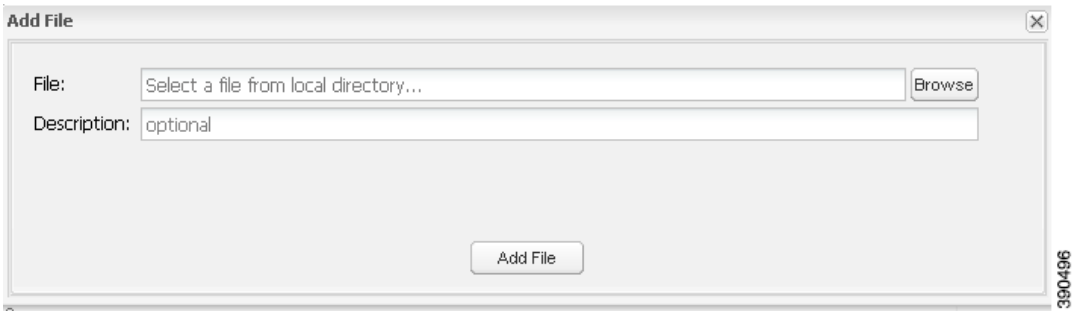
2. [Add File] をクリックし、ファイルの場所を検索します

(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。

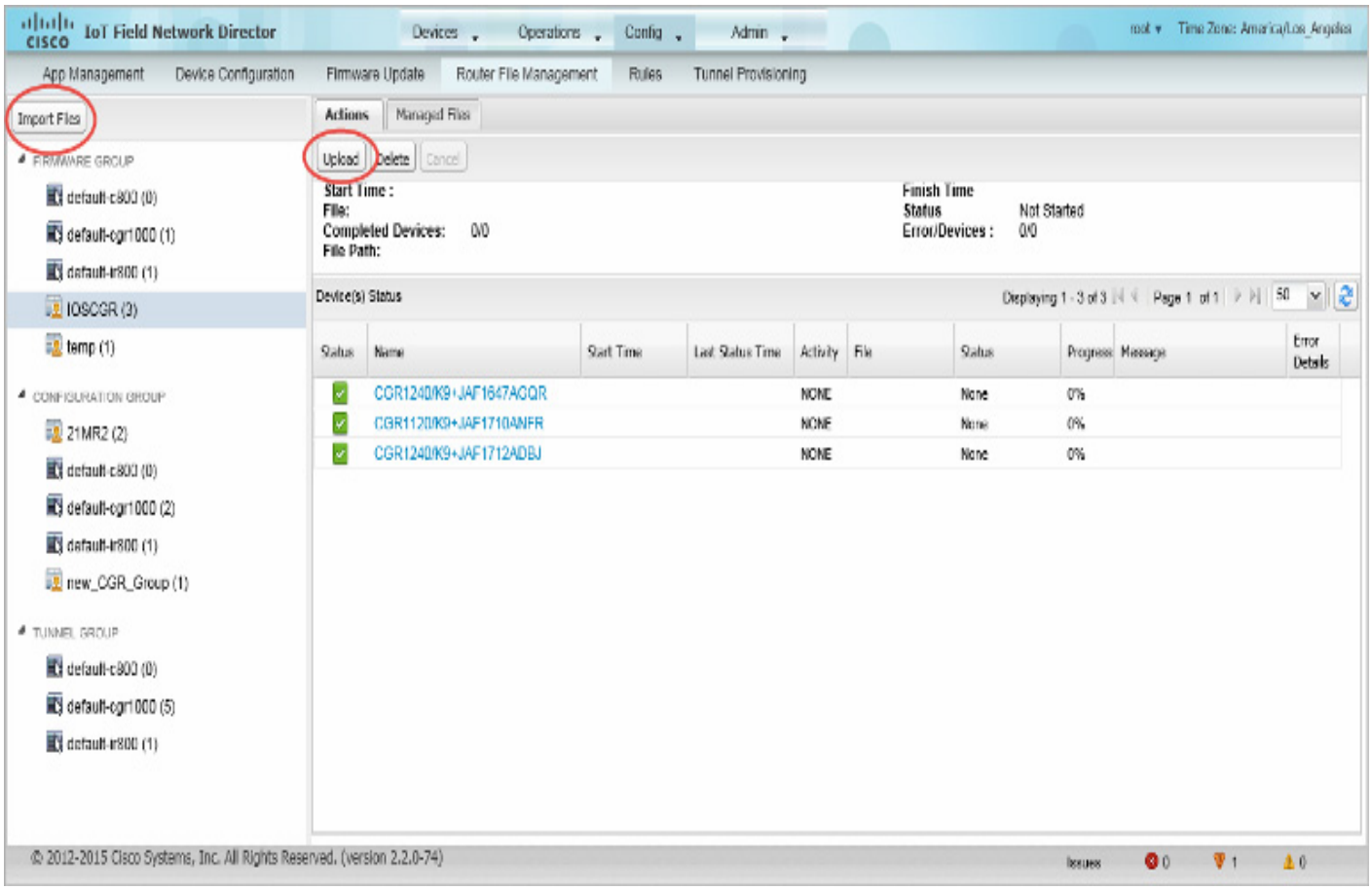
5. ステップ 2 から 4 を繰り返して他のファイルを追加するか、ファイル転送 を参照して選択したデバイスまたはグループにファイルをアップロードするか、または [Select File From List] ダイアログボックスを閉じます。

ファイル転送

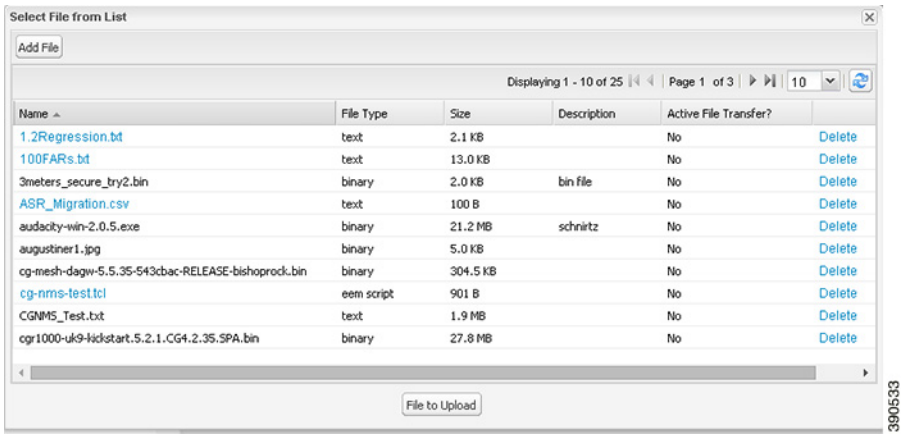
NMS データベースからファームウェア グループ、設定グループ、トンネル プロビジョニング グループ、または個々の FAR にファイルを転送できます。インポート ファイルの最大サイズは 200 MB です。

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。

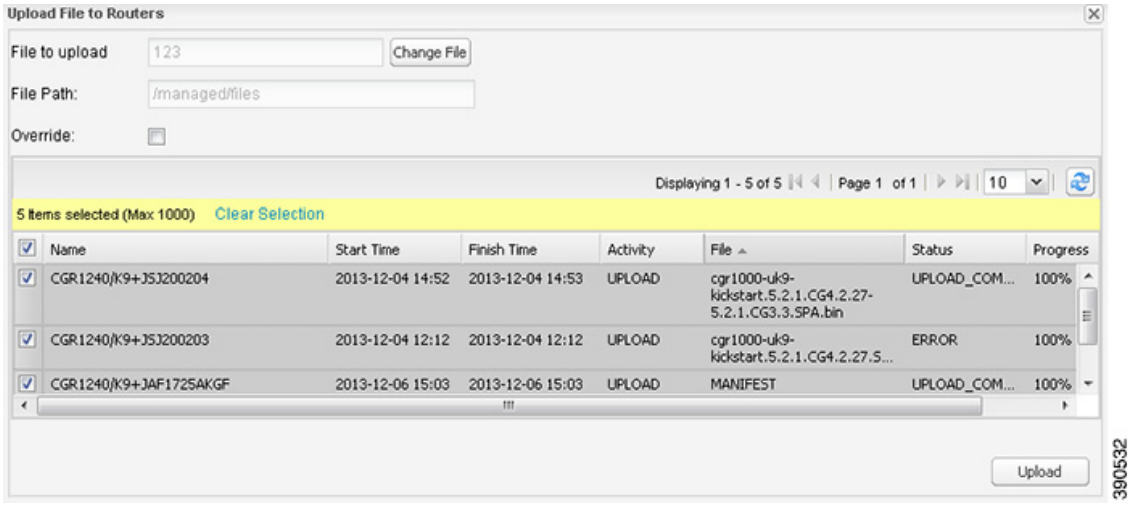


[Select File from List] ダイアログボックスが表示されます。



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。

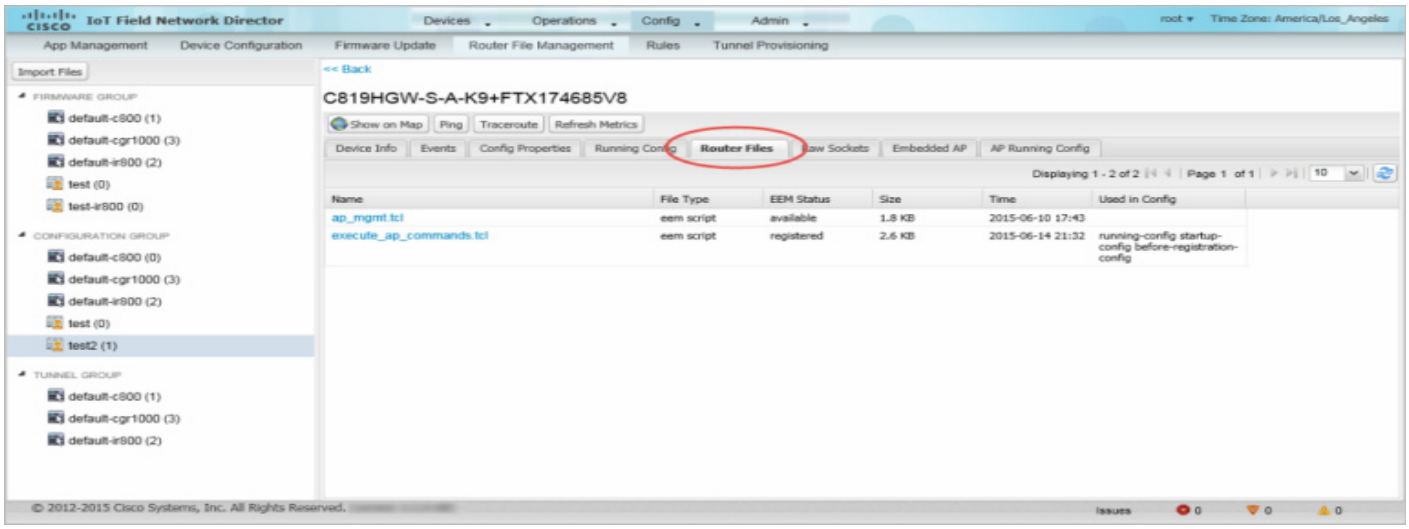
IoT FND から転送されるすべてのファイルは、Cisco IOS CGR では flash:/managed/files/、CG-OS CGR では bootflash:/managed/files/ 内の FAR に置かれます。

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

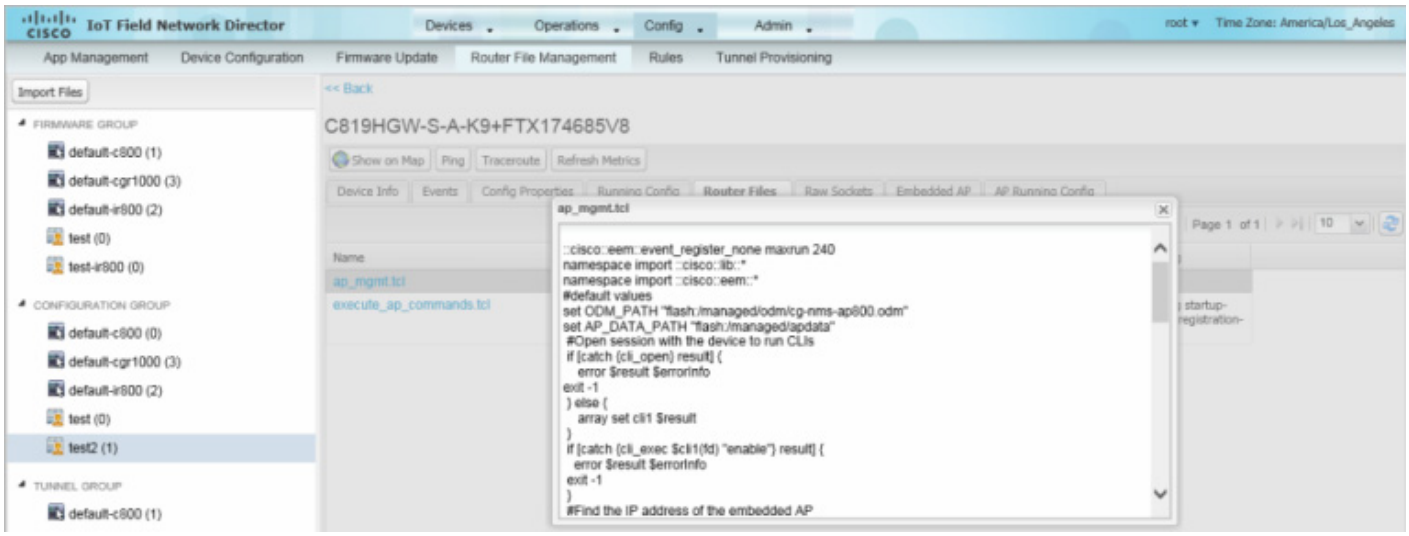
インポートされたテキスト ファイルの内容を表示するには、次の手順を実行します。

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。

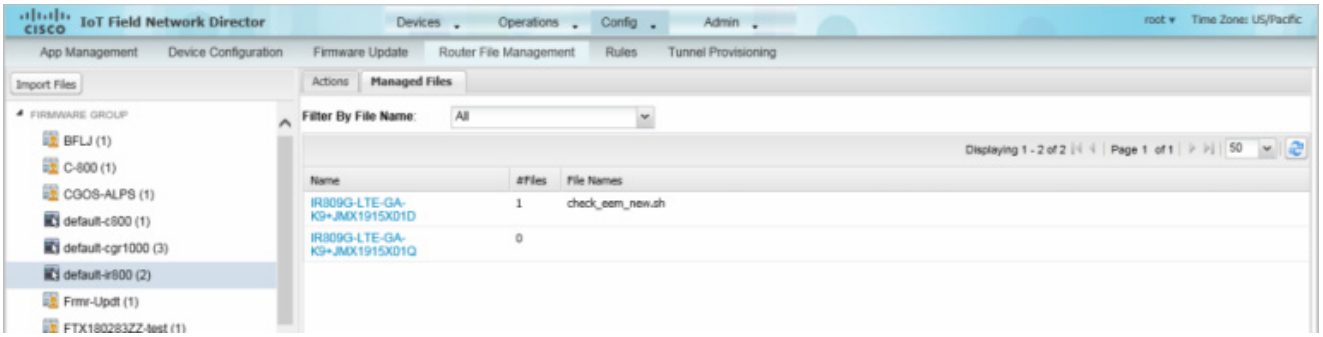
   (注) IoT FND は、100 KB 未満のプレーン テキストとして保存されているファイルのみを表示します。これより大きいテキスト ファイル、およびサイズに関係なくバイナリ ファイルは表示できません。それらのファイル タイプはハイパーリンクになりません。



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。

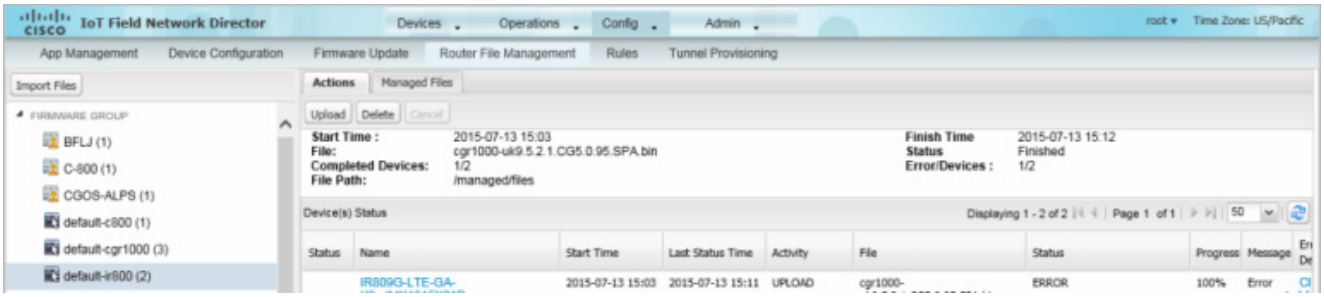
- [Device Info] ページへの EID リンク
- デバイスに保存されているファイルの数
- アップロードされているファイルの名前

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。

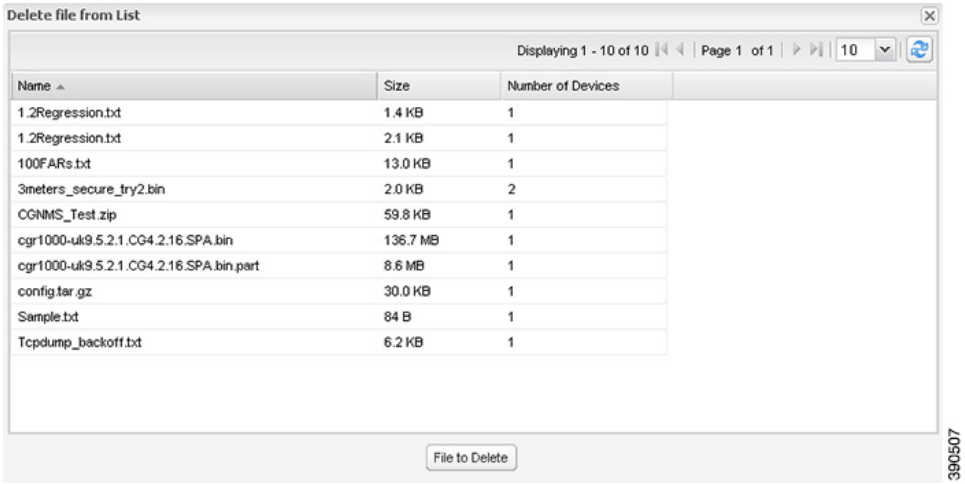
- 最後の転送の開始日時
- 最後の転送の終了日時
- ファイル名
- プロセスのステータス：UNKNOWN、AWAITING_DELETE、DELETE_IN_PROGRESS、DELETE_COMPLETE、CANCELLED、NOTSTARTED、UPLOAD_IN_PROGRESS、UPLOAD_COMPLETE、STOPPING、STOPPED
- アップロードが完了したデバイスの数とターゲット デバイスの合計数
- エラーの数とエラーが発生したデバイスの数
- ファイル パス

- [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。

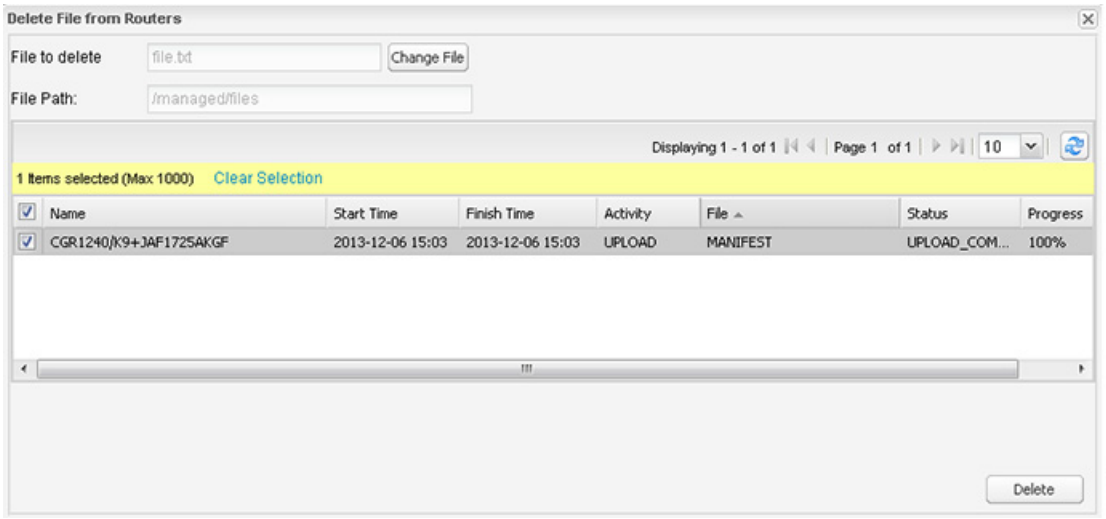
1. [Config] > [Router File Management] ページの [Browse Devices] ペインで、ファイルの転送先のグループを選択します。
2. [Actions] タブで [Delete] を選択します。
3. [Delete file from List] ダイアログで、削除するファイルを選択します。



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。

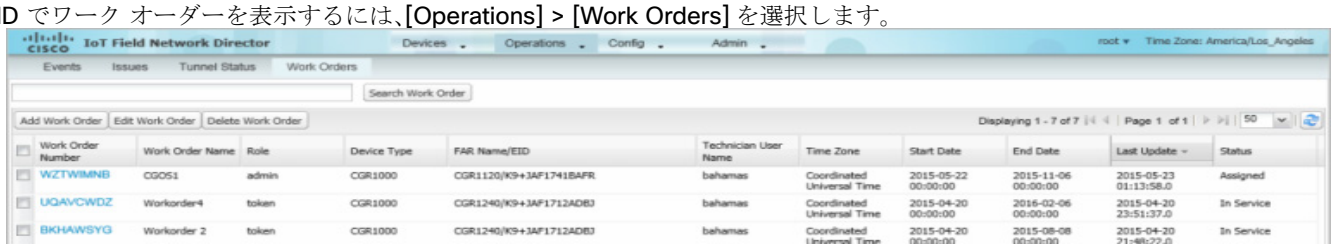


表 9 に、[Work Orders] ページに表示するフィールドを示します。

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

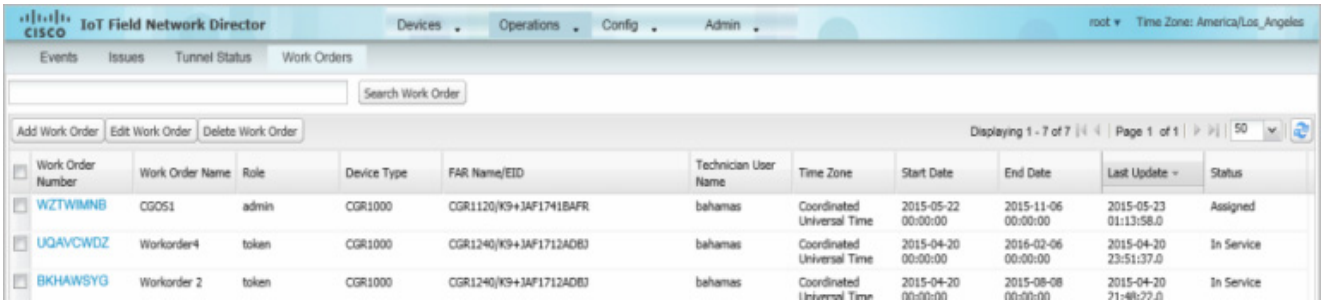
- ユーザ アカウントで、[Work Order Management] 権限が有効になっている必要があります。
- IoT DM への要求に署名済みワーク オーダーを提供するには、エイリアス cgms を使用して、cgms_keystore に IoT DM 証明書をインポートする必要があります。
- フィールド技術者のユーザ アカウントを作成します。（Device Manager（IoT-DM）ユーザのユーザ アカウントの作成を参照）。

（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。

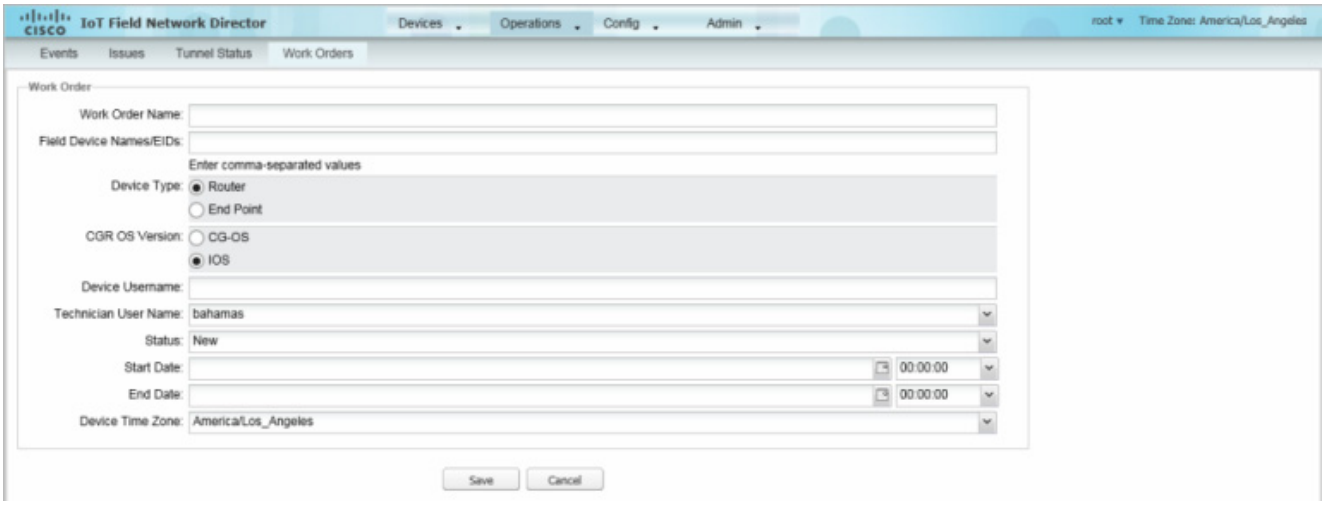
手順の詳細

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]

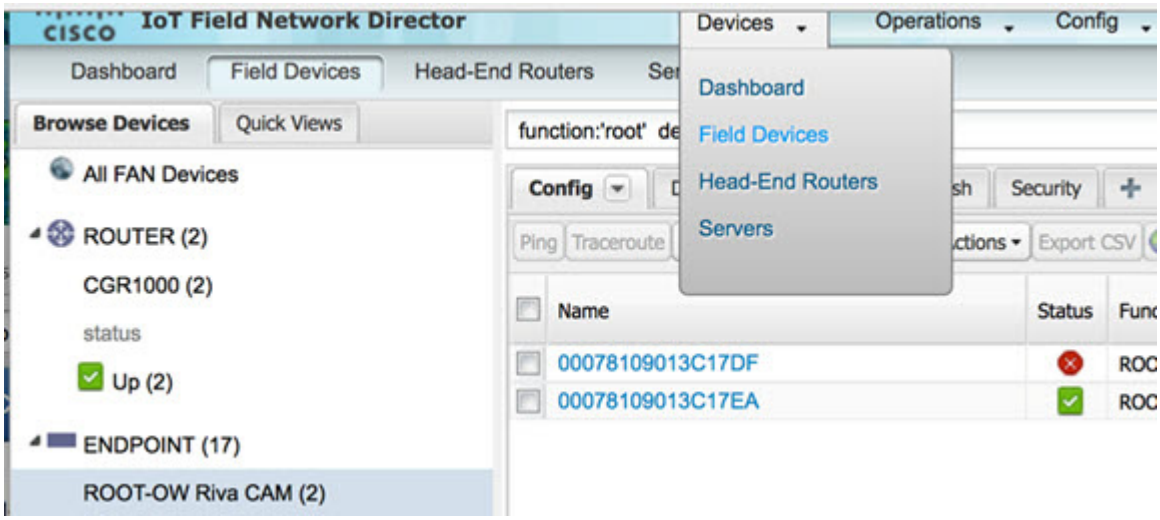
表 20 に、[Head-End Routers] > [Config Properties] ページの [Tunnel 2 Config] エリア内のフィールドを示します。

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。

ファームウェア アップグレードの管理

ここでは、IoT FND におけるファームウェア アップグレードの設定の管理について説明します。具体的な内容は次のとおりです。

IoT FND を使用して、FAR（CGR1000、C800、IR800）、AP800、メッシュ エンドポイント（CGE および Range Extender）で実行されているファームウェアをアップグレードします。IoT FND は、後で IoT FND および IoT DM ファイル転送を通じてファームウェア グループ内の FAR に転送するため、および IoT FND を使用して ME に転送するため、ファームウェア バイナリをそのデータベースに保存します。

シスコではファームウェア バンドルを zip ファイルとして提供しています。Cisco IOS では、ソフトウェア バンドルにハイパーバイザ、システム イメージ、および IOx イメージ（ゲスト OS、ホスト OS など）が含まれています。Cisco CG-OS では、IoT FND により、バンドルに含まれるキックスタートとシステム イメージが自動的に解凍されます。ファームウェア システム イメージはサイズが大きく（約 130 MB）、キックスタート イメージは約 30 MB です。すべてのファームウェア バンドルには、マニフェスト ファイルとバンドル内のイメージに関するメタデータが含まれています。アップロード プロセスは一時停止、停止、または再開できます。

FAR ファームウェアのアップデート

IoT FND では次の 2 ステップで FAR ファームウェアをアップデートします。

1. IoT FND からデバイスにファームウェア イメージをアップロードします。

   ファームウェア イメージのサイズが大きいため、インターフェイスの速度によっては、FAR へのアップロードに 30 分程かかります。

2. デバイスにファームウェアをインストールしてリロードします。

(注) インストール プロセスを開始する必要があります。イメージのアップロード後に、IoT FND によってプロセスが自動的に開始されることはありません。

トンネル プロビジョニングの登録と要求のために FAR が IoT FND に初めてコンタクトすると、IoT FND は FAR をデフォルトの工場出荷時の設定（ps-start-config）にロールバックしてから、新しいファームウェア イメージのアップロードとインストールを行います。

(注) このロールバックには、ps-start-config でブート パラメータを更新し、最新の設定を適用するために 2 回目のリロードが必要になります。この 2 回目のリロードにより、インストールおよびリロードの操作にさらに 10 ～ 15 分程かかります。

ゲスト OS イメージのアップグレード

CGR の工場出荷時の設定によっては、ゲスト OS（GOS）が VM インスタンス内に存在している場合があります。Cisco IOS のインストールまたはアップグレードは、[Config] > [Firmware Update] ページでできます（「FAR ファームウェアのアップデート」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。

任意の Cisco IOS をインストールまたはアップグレードすると、IoT FND が GOS を検出した際に、初期通信が設定されていることを確認してから、必要な設定を行います。CGR が IP アドレスを提供し、GOS のゲートウェイとして機能するには、DHCP プールがあり、GigabitEthernet 0/1 インターフェイスが設定されている必要があります。新しい GOS イメージによって既存の設定が上書きされます。IoT FND には、既存のアプリをアップグレードされたゲスト OS に移植する内部バックアップと復元メカニズムがあります（「ゲスト OS の管理」を参照）。

CGR の設定の詳細については、『*Cisco 1000 Series Connected Grid Routers Configuration Guides*』を参照してください。

(注) IoT FND が VM に Cisco 以外の OS がインストールされていることを検出すると、ファームウェア バンドルはアップロードされず、シスコ参照 GOS はインストールされません。

WPAN イメージのアップグレード

[Config] > [Firmware Update] ページで、他のイメージのアップグレードと同じように、[Images] サブタブ（左側）と [Upload Image] ボタンを使用して、独立した WPAN イメージ（IOS-WPAN-RF または IOS-WPAN-PLC）を IoT FND にアップロードできます。このプロセスは「統合されていない WPAN ファームウェア アップグレード」と呼ばれます。

IOS CGR イメージ オプションと統合された WPAN ファームウェア イメージはまだサポートされています。

また、IOS イメージにバンドルされたイメージから WPAN ファームウェアのみアップグレードしたい場合（たとえば、IOS のアップグレード時に WPAN ファームウェア アップグレード オプションがオンになっていなかった場合）は、各 WPAN イメージのタイプ（IOS-WPAN-RF または IOS-WPAN-PLC）の下に [Install from Router] オプションも提供されます。

詳細なステップについては、FAR ファームウェア イメージの使用、268 ページを参照してください。

アクションの有効期限タイマーの変更

cgnms_preferences.sh スクリプトを使用して、IoT FND データベース内のアクションの有効期限タイマーを設定または取得することができます。

```
/opt/cgms
/bin/cgnms_preferences setCgrActionExpirationTimeout 50
```

有効なオプションは次のとおりです。

- set*<pkg>actionExpirationTimeoutMins<value>*

  値は次のとおりです。

  - *<pkg>* はプリファレンス パッケージです（*set* および *get* の操作に必要）。
  - *actionExpirationTimeoutMins* はプリファレンス キーです（*set* および *get* の操作に必要）。
  - *<value>* は分単位の優先値です（*set* および *setCgrActionExpirationTimeout* の操作に必要）。
- setCgrActionExpirationTimeout *<value>*
- get*<pkg>actionExpirationTimeoutMins*
- *getCgrActionExpirationTimeout*

例

次の例では、アクション タイマー値を取得、設定し、現在の値を再度取得し、値を削除し、null 値を取得します。

```
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:42,004:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
5
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh setCgrActionExpirationTimeout 50
2013-08-12 22:38:51,907:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh getCgrActionExpirationTimeout
2013-08-12 22:38:58,591:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:12,921:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
50
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh set com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins 15
2013-08-12 22:39:23,594:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
Successfully set the preferences.
[root@userID-lnx2 cgms]# ./dist/cgms-1.x/bin/cgnms_preferences.sh get com.cisco.cgms.elements.ciscocgr
actionExpirationTimeoutMins
2013-08-12 22:39:29,231:INFO:main:CgmsConnectionProvider: registered the database url for CG-NMS:
[jdbc:oracle:thin:@localhost:1522:cgms]
15
```

メッシュ エンドポイント ファームウェアのアップデート

IoT FND にファームウェア イメージを ME ファームウェア グループまたはサブネットのメンバーにアップロードするように指示すると、IoT FND はバックグラウンドでそのイメージをグループ メンバーにプッシュして、アップロードの進捗を追跡し、デバイスがイメージを確実に受け取れるようにします。

メッシュ エンドポイントは次の 3 つのファームウェア イメージを保存します。

- アップロードされたイメージ:最後にアップロードされたイメージ
- 動作しているイメージ:現在動作しているイメージ
- バックアップ イメージ:動作しているイメージに問題がある場合に、エンドポイントのゴールデン(フォールバック)イメージとして機能します。

(注)最大 3 つのファームウェアのダウンロードを同時に開始できます。

メッシュ ファームウェアの移行(CG-OS CG4 プラットフォームのみ)

(注)Cisco Mesh へのメッシュ ファームウェアの移行は、CG-OS バージョン CG4(4) を実行する CGR ではサポートされません。

IoT FND では、CGR ファームウェアの旧バージョンを更新して、次の IoT FND North Bound API を使用して Cisco Mesh のネットワークを許可することができます。

- findEidByIpAddress
- startReprovisionByEidList

- startReprovisionByEidListAbridged
- startReprovisionByGroup
- startReprovisionByGroupAbridged

使用方法ついては、『*Cisco Connected Grid NMS North Bound API Programming Guide*』を参照してください。

ファームウェア グループの設定

ここでは、ファームウェア グループの追加、削除、および設定方法について説明します。具体的な内容は次のとおりです。

- ファームウェア グループの追加ファームウェア グループの追加
- ファームウェア グループへのデバイスの割り当て
- ファームウェア グループの名前変更
- ファームウェア グループの削除

(注)アップロード操作は、[Resume] ボタンをクリックした場合にのみ開始されます。

FAR または ME を IoT FND に追加すると、アプリケーションによってデバイスが対応するデフォルトのファームウェア グループ(default-*<router>* または default-cgmesh)にソートされます。これらのグループを使用して、ファームウェア イメージをメンバーのデバイスにアップロードおよびインストールします。ファームウェア グループを追加して、デバイスのカスタム セットを管理します。ファームウェア グループへのデバイスの割り当ては、手動または一括で行えます。ファームウェア グループを削除する前に、グループ内のすべてのデバイスを別のグループに移動する必要があります。空ではないグループを削除することはできません。

(注)ファームウェア グループを作成するときには、次の警告に注意してください。

- CGR、IR800、および C800 は、ネットワーク上に共存することはできますが、ファームウェア管理では、これらが同じファームウェア グループに属することはできません。
- IR500 とその他のメッシュ エンドポイント デバイスは、ネットワーク上に共存することはできますが、ファームウェア管理では、これらが同じグループに属することはできません。

[Config] > [Firmware Update] ページの [Groups] タブには、さまざまなデバイスのメトリックが表示されます。

IoT FND は、選択したファームウェア グループ内の FAR にイメージに関するこの情報を表示します。

フィールド	説明
Selected Firmware Image	グループ メンバーにアップロードされる現在のイメージの zip アーカイブまたはイメージの名前。
Current Action	実行されるファームウェア アクションの名前。
Current Status	アップロード中のイメージのステータス。次のようなステータスがあります。 ■ Image Loading、Upload Paused、Upload Stopped、Upload Finished、Upload Stopping、Upload Pausing ■ Scheduling Reload、Reload Paused、Reload Stopped、Reload Scheduling Finished、Reload Stopping、Reload Pausing ■ Setting Backup、Backup Paused、Backup Stopped、Backup Finished、Backup Stopping、Backup Pausing

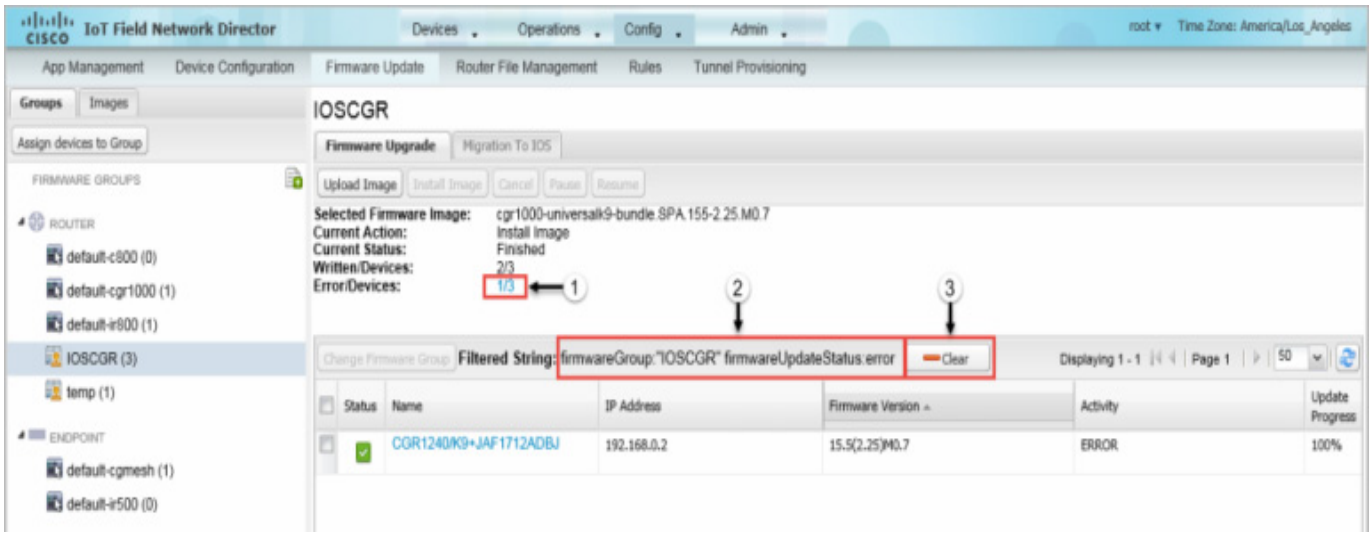
フィールド	説明
Written/Devices	グループ内のデバイスの総数のうち、イメージを受け取るまたはイメージをインストールするデバイスの数を指定します。 たとえば 1/3 は、グループ内の 3 つのデバイスのうち、1 つのデバイスがファームウェア イメージを受け取ったことを意味します。
Error/Devices	グループ内のデバイスの総数のうち、イメージを受け取るまたはイメージをインストールするのに失敗したデバイスの数を指定します。たとえば 2/3 は、グループ内の 3 つのデバイスのうち、2 つのデバイスがイメージのインストールに失敗したことを意味します。 ヒント:エラー状態にあるデバイスを表示するには、[Error/Devices] リンク(図 1 の 1)をクリックします。

IoT FND はグループ内のすべての FAR に対してこの情報を表示します。

フィールド	説明
Status(ステータス)	デバイスのステータス(Up、Down、または Unheard など)。
名前	デバイスの EID。
IP アドレス	デバイスの IP アドレス。
Firmware Version	デバイスにインストールされたファームウェア イメージのバージョン。
アクティブな状態	デバイス アクティビティ。
Update Progress	ファームウェア イメージ更新の進捗状況。100% の進捗状況は、イメージのアップロードが完了したことを示します。
Last Firmware Status Heard	最後に確認されたファームウェア ステータス。
エラー メッセージ	イメージのアップロードに失敗した場合のエラー メッセージ。
Error Details	選択したデバイスのエラーの詳細が表示されます。

ヒント:フィルタを適用(3)するには、[Error/Devices] リンク(図 1 の 1)をクリックします。選択したデバイス グループのフィルタされていないビューに戻すには、[Clear] ボタン(2)をクリックします。

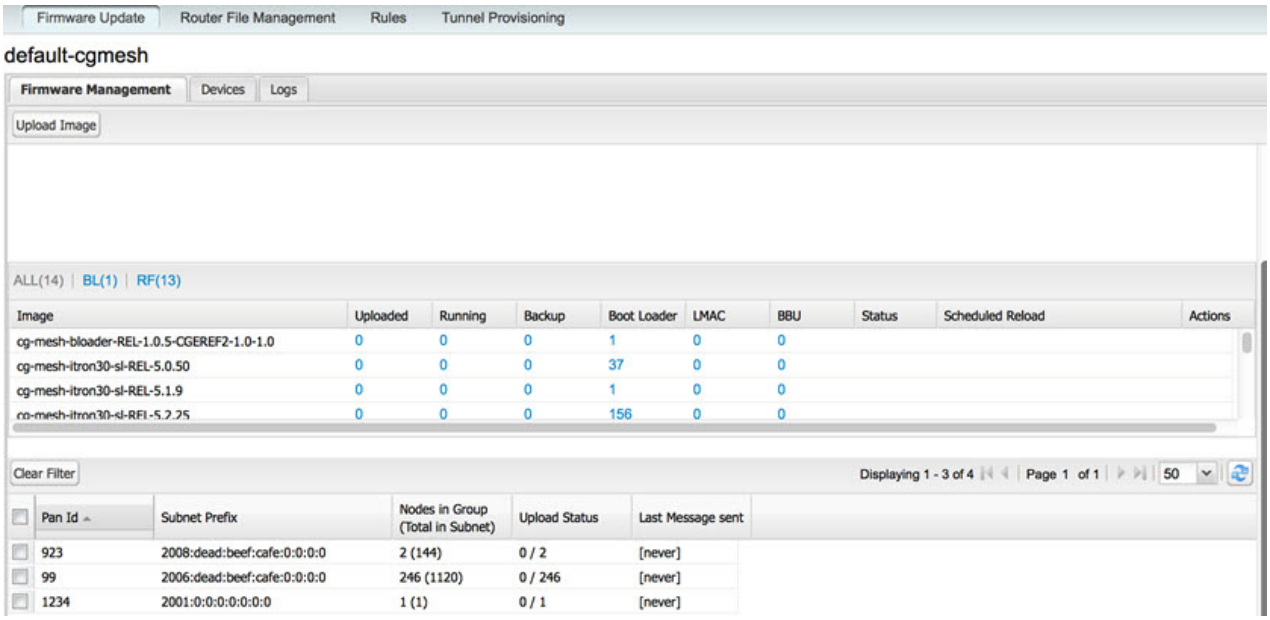
図 1　[Firmware Update] ページ:エラーが発生したデバイス



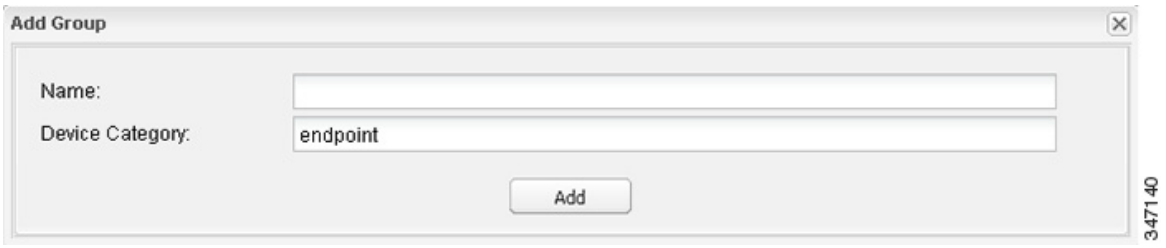
ファームウェア グループの追加

ファームウェア グループを追加するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。



3. [FIRMWARE GROUPS] ペインで、[default-cgr1000]、[default-c800]、[default-ir500]、[default-ir800]、または [default-cgmesh] を選択します。
4. [FIRMWARE GROUPS] ペインの右上の [Add Group]( ) をクリックします。
5. [Add Group] ダイアログ ボックスに、ファームウェア グループの名前を入力します。[Device Category] は、3. で選択したデバイス タイプによって異なります。



6. [Add] をクリックします。

   新しいグループ ラベルが、[FIRMWARE GROUPS] ペインの対応するデバイス タイプの下に表示されます。

新しいグループにデバイスを割り当てるには、「ファームウェア グループへのデバイスの割り当て」を参照してください。

ファームウェア グループへのデバイスの割り当て

ここでは、デバイスの移動について説明します。具体的な内容は次のとおりです。

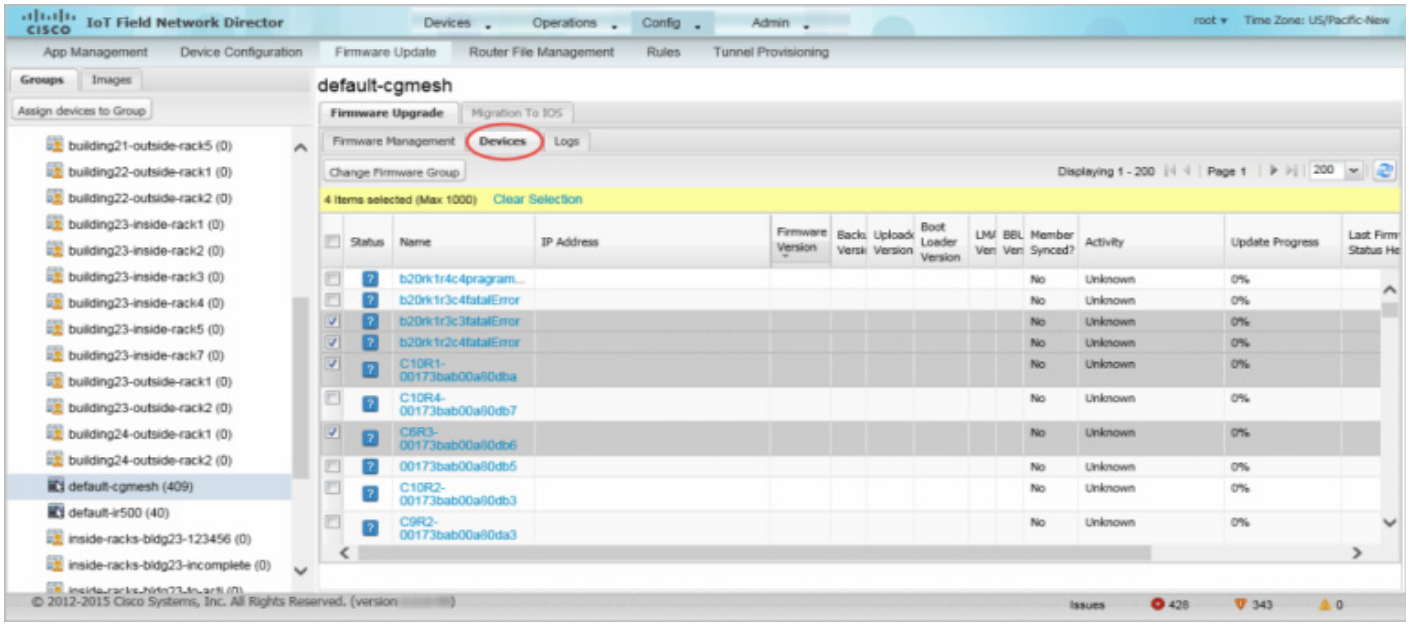
- 他のグループにデバイスを手動で移動する
- 他のグループにデバイスを一括で移動する

他のグループにデバイスを手動で移動する

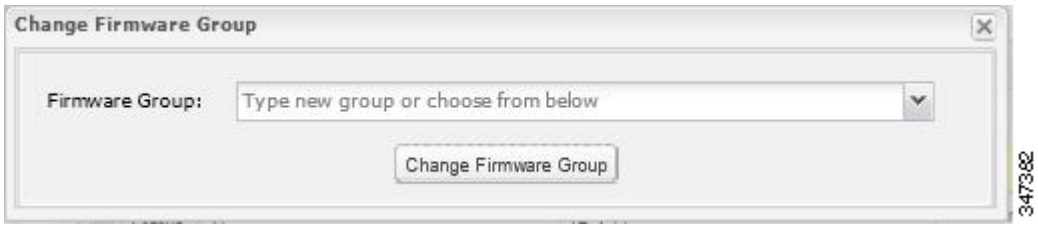
グループに手動でデバイスを移動するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、デバイス タイプに基づいて、目的のファームウェア グループを選択します。

   (注) これが ENDPOINT ファームウェア グループの場合は、メイン ペインの上部にある [Devices] タブをクリックします。



4. 移動するデバイスのチェック ボックスをオンにします。
5. [Change Firmware Group] をクリックします。



6. [Firmware Group] ドロップダウン メニューから、デバイスの移動先のファームウェア グループを選択するか、新しいグループ名を入力します。
7. [Change Firmware Group] をクリックします。
8. [Close] をクリックします。

他のグループにデバイスを一括で移動する

グループ間でデバイスを一括で移動するには、次の手順を実行します。

1. 次の例に示す形式を使用して、移動するデバイスをリストした CSV ファイルまたは XML ファイルを作成します。

CGR の *デバイス タイプ/EID*:

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

***EID*（ME 専用）:**

```
eid
00078108003c1e07
00078108003C210b
```

***EID*（IR800 専用）:**

```
eid
ir800
```

***EID*（ISR 800 専用）:**

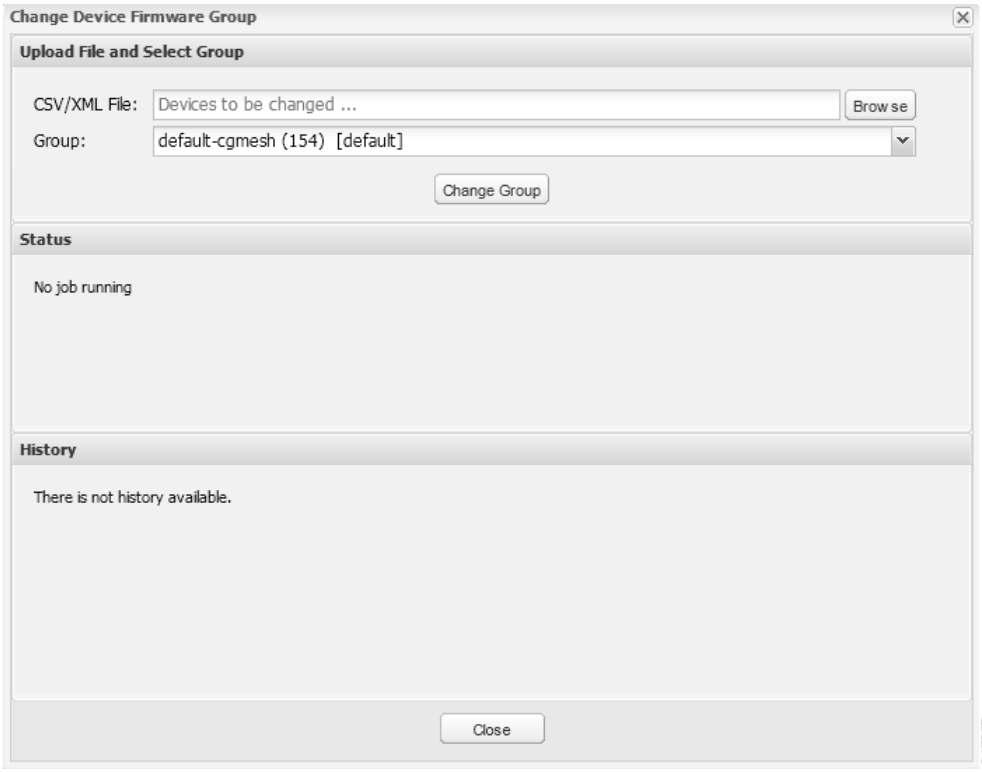
```
eid
C819HGW-S-A-K9+FTX174685V0
C819HGW-S-A-K9+FTX174686V0
C819HGW-S-A-K9+FTX174687V0
```

***EID*（IR500 専用）:**

```
eid
da1
da2
da3
```

(注) ファイルごとに 1 つのデバイス タイプのみをリストできます。

2. [Config] > [Firmware Update] の順に選択します。
3. [Groups] タブをクリックします。
4. [Assign Devices to Group] をクリックします。



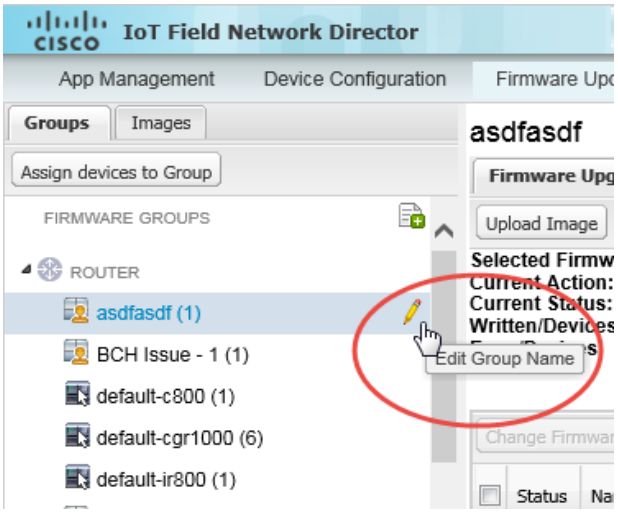
5. [Browse] をクリックして、デバイス リストの CSV ファイルまたは XML ファイルを参照します。
6. [Group] ドロップダウン メニューから、目的のグループを選択します。
7. [Change Group] をクリックします。

   IoT FND はファイルにリストされているデバイスを現在のグループから目的のグループに移動します。
8. [Close] をクリックします。

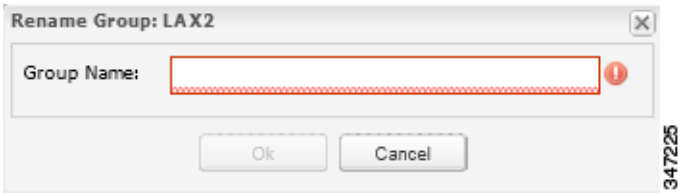
ファームウェア グループの名前変更

ファームウェア グループを名前変更するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、名前変更するファームウェア グループを選択します。
4. グループの上にカーソルを移動し、[Edit Group Name] の鉛筆アイコンをクリックします。



5. [Rename Group] ウィンドウで、新しい名前を入力して [OK] をクリックします。



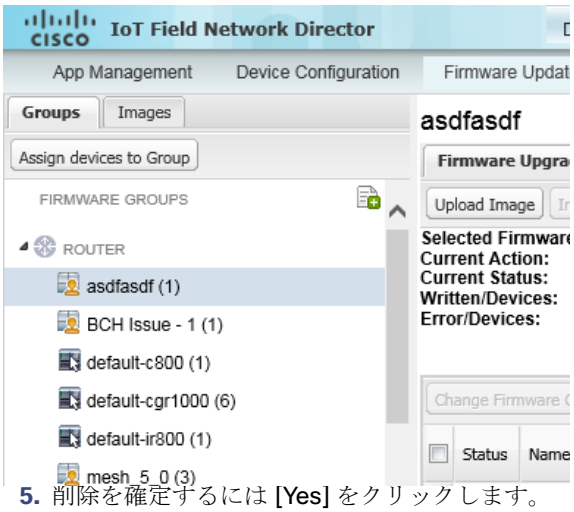
(注) 上の図のように、フィールド内に無効な文字エントリ（@、#、!、+ など）を入力すると、IoT FND では赤いアラート アイコンが表示され、フィールドが赤で強調表示され、[OK] ボタンが無効化されます。

ファームウェア グループの削除

(注) ファームウェア グループを削除する前に、グループ内のすべてのデバイスを別のグループに移動する必要があります。空ではないグループを削除することはできません。

ファームウェア グループを削除するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、削除するファームウェア グループを選択します。
4. グループの上にカーソルを移動し、[Delete]（−）をクリックします。



5. 削除を確定するには [Yes] をクリックします。
6. [OK] をクリックします。

FAR ファームウェア イメージの使用

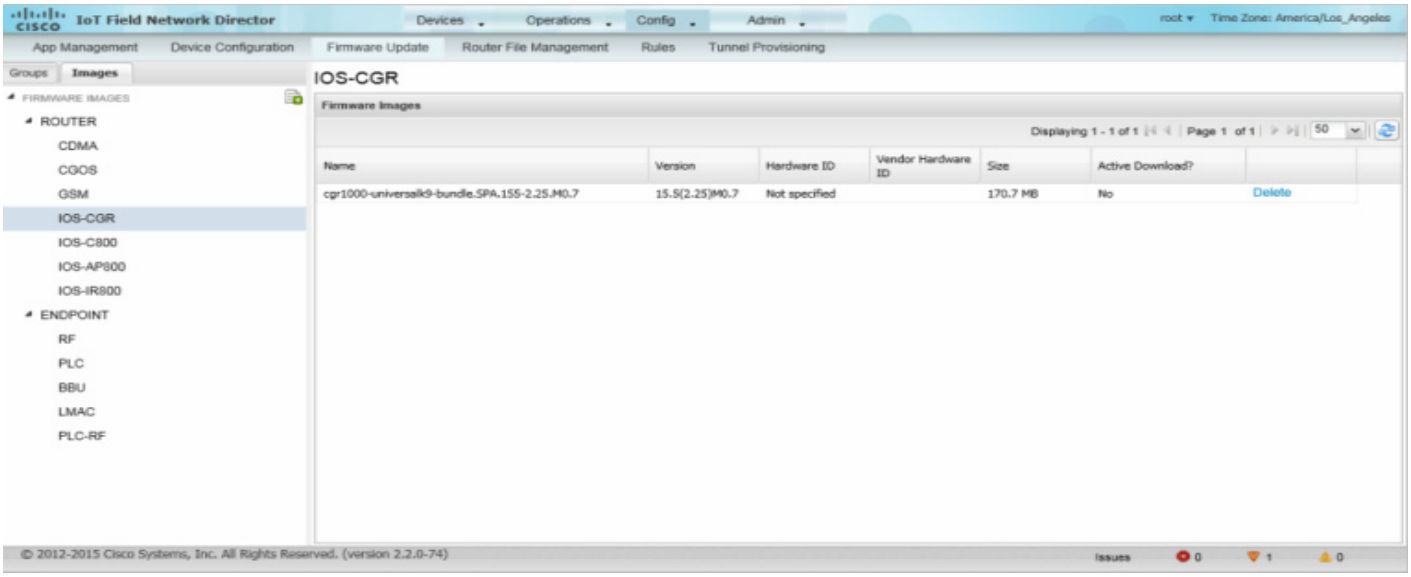
ここでは、FAR ファームウェア イメージを IoT FND に追加する方法と、FAR にイメージをアップロードおよびインストールする方法について説明します。具体的な内容は次のとおりです。

- IoT FND でのファームウェア イメージ ファイルの表示
- IoT FND へのファームウェア イメージの追加
- FAR グループへのファームウェア イメージのアップロード
- FAR ファームウェア イメージのアップロードのキャンセル
- FAR ファームウェア イメージのアップロードの一時停止と再開
- ファームウェア イメージのインストール
- ファームウェア イメージのインストールの停止
- FAR ファームウェア イメージのインストールの一時停止と再開
- ファームウェア イメージのインストール、およびその他のアクションからサブネットを除外する

IoT FND でのファームウェア イメージ ファイルの表示

[Config] > [Firmware Update] ページの [Images] ペインからのファームウェア イメージ情報を表示できます。[ROUTER] または [ENDPOINT] を選択し、IoT FND データベース内のこれらのデバイスのすべてのファームウェア イメージを表示します。表示を改善するファームウェア イメージのタイプを選択します。たとえば、図 2 には、[ENDPOINT] > [BBU] が選択され、使用可能な BBU ファームウェア イメージ ファイルの名前とバージョン、サポートされるハードウェア ID が表示されています。

図 2　[Config] > [Firmware Update Images] ペイン



IoT FND はリスト内のすべてのイメージに対し、この情報を提供します。

フィールド	説明
名前	ファームウェア イメージ バンドルのファイル名。
Version	ファームウェア バンドルのバージョン。
ハードウェア ID	このイメージをダウンロードできるハードウェア ファミリ。
サイズ	ファームウェア バンドルのサイズ。
Active Download	ファームウェア イメージを使用しているアクティブなファームウェア。

IoT FND へのファームウェア イメージの追加

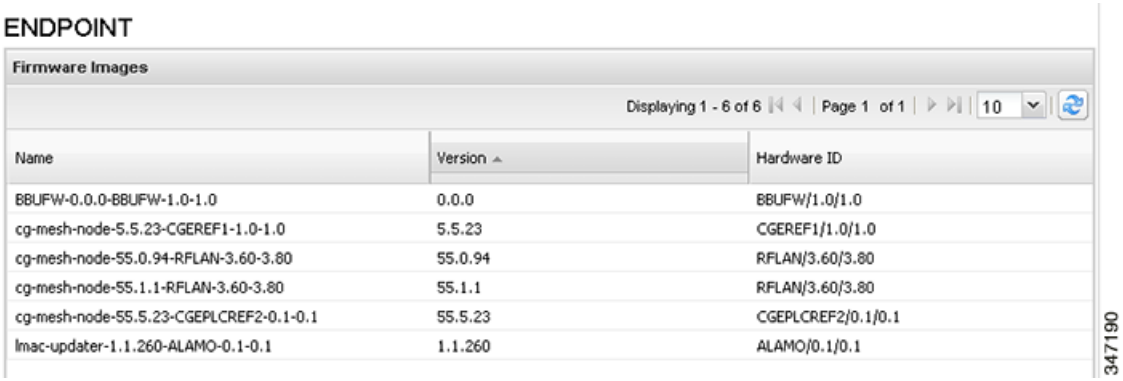
ファームウェア イメージをデバイスにアップロードしてインストールするには、先にイメージ ファイルを（zip アーカイブとして）IoT FND に追加する必要があります。IoT FND はイメージを自身のデータベースに保存します。

（注）イメージ ファイルは解凍しないでください。IoT FND によりファイルが解凍されます。

IoT FND にファームウェア イメージを追加するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Images] タブをクリックします（図 2）。
3. [Firmware Images] ペインで、[ROUTER] または [ENDPOINT] と、デバイス グループのタイプを選択します。
4. [Add Image]（ ）をクリックします。
5. [Browse] をクリックして、ファームウェア イメージを見つけます。イメージを選択し、[Choose] をクリックします。
6. [Upload] をクリックします。

   イメージが [Firmware Images] ペインに表示されます。



- イメージを削除するには、[Delete] リンクをクリックします。確認のために [Yes] をクリックします。

  ダウンロードが進行中のファームウェア イメージ（[Active Download?] 列が [Yes] になっている）は、削除できません。
- ファームウェア イメージをグループ内のデバイスにアップロードするには、グループを選択してから、[Upload Image] をクリックします。FAR グループへのファームウェア イメージのアップロードを参照してください。

FAR グループへのファームウェア イメージのアップロード

ファームウェア イメージを FAR ファームウェア グループ メンバーにアップロードすると、IoT FND はバックグラウンドでそのイメージをグループ メンバーにプッシュして、アップロードの進捗を追跡し、デバイスがイメージを確実に受け取れるようにします。

FAR では、ファームウェア イメージのアップロードおよびインストールには 200 MB の空きディスク領域が必要です。IoT FND はイメージ ファイルを FAR の .../managed/images ディレクトリに保存します。

(注) FAR にファームウェア イメージのための十分なディスク領域がない場合、IoT FND は FAR でディスクのクリーンアップ プロセスを開始して、新しいイメージをアップロードするのに十分なディスク領域ができるまで、次のファイルを順次削除します。

- 現在実行されていない、または IOS CGR の before-tunnel-config、before-registration-config、express-setup-config、および factory-config ファイル、CG-OS CGR の golden-config、ps-start-config、express-setup-config、または factory-config で参照されていない .../managed/images ディレクトリ内の未使用のファイル
- CG-OS CGR の bootflash ディレクトリの未使用の .gbin ファイルと .bin ファイル

それでも十分な領域が確保できない場合は、FAR の未使用のファイルを手動で削除する必要があります。

ファームウェア イメージを FAR グループ メンバーにアップロードするには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、更新するファームウェア グループを選択します。

   (注) CGR グループには、Cisco IOS および CG-OS を実行しているデバイスを含めることができます。したがって、Cisco IOS ソフトウェア イメージは、Cisco IOS を実行しているデバイス（IR800、ISR800、CGR）にのみアップロードします。CG-OS イメージを受け入れるのは CGR だけです。

   IoT FND はルータに適用可能なファームウェア イメージのタイプを表示します。

Image	タイプ	適用可能なデバイス
CDMA	all	Cisco IOS CGR、IR800、ISR800
CGOS	cgr1000	ゲスト OS を実行している Cisco IOS CGR

Image	タイプ	適用可能なデバイス
GSM	all	Cisco IOS CGR、IR800、ISR800
IOS-CGR	cgr1000	Cisco IOS CGR（CGR 1240 および CGR 1120）
IOS-C800	c800	Cisco 800 シリーズ ISR が接続されたデバイス。
IOS-AP800	ap800	Cisco 800 シリーズ アクセス ポイント。
IOS-IR800	ir800	Cisco 800 シリーズ ISR。
IOS-WPAN-RF	cgr1000	Cisco IOS-CGR
IOS-WPAN-PLC	cgr1000	Cisco IOS-CGR
LORAWAN	lorawan	Cisco IR829-GW

4. [Upload Image] をクリックして、エントリ パネルを開きます。
5. [Select Type:] ドロップダウン メニューから、使用中のデバイスのファームウェア タイプを選択します。
6. [Select an Image:] ドロップダウン メニューから、アップロードするファームウェア バンドルを選択します。

   一部の IOS-CGR ソフトウェア バンドルについては、次のいずれかのオプションを選択することもできます。

   - このバンドルからゲスト OS をインストールする
   - このバンドルから WPAN ファームウェアをインストールする
7. [Upload Image] をクリックします。
8. [OK] をクリックします。

IoT FND によりアップロード プロセスが開始されます。イメージのアップロード後、「ファームウェア イメージのインストール」の説明に従ってイメージをインストールします。

FAR ファームウェア イメージのアップロードのキャンセル

ファームウェア ルータ グループへのイメージのアップロード プロセスは、いつでも停止できます。アップロードの停止には数分かかることがあります。イメージのアップロードをキャンセルすると、イメージのアップロード プロセスは、現在実行中のタスクをすぐに停止して、キューに入っているすべてのタスクをブロックします。

(注) 実行中のタスクは完了せず、ファイルの一部がディスクに残り、アップロード操作を完了するまで、ファームウェア グループのステータスは「CANCELING」に設定されます。

グループへのファームウェア イメージのアップロードを停止するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、ファームウェア グループを選択します。
4. [Cancel] をクリックします。
5. [Yes] をクリックします。

FAR ファームウェア イメージのアップロードの一時停止と再開

FAR ファームウェア グループへのイメージのアップロード プロセスは、いつでも一時停止・再開することができます。

(注)イメージのアップロード プロセスは、すぐに停止されることはありません。キューに入っている(ただし実行されていない)すべての操作は一時停止されますが、現在実行中のタスクは完了します。ステータスは、アクティブな操作が完了するまで「PAUSING」に変更されます。

ファームウェア イメージのアップロードを一時停止するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、ファームウェア グループを選択します。
4. [Pause] をクリックします。

   アクティブなアップロード操作が完了するまで、[Status] 列に「PAUSING」が表示されます。[Resume] ボタンをクリックするまで、新しいアップロード操作は開始されません。
5. [Yes] をクリックします。

アップロード プロセスを再開するには、[Resume] をクリックします。

(注)ファームウェア イメージをデバイスにアップロード中に IoT FND サーバがダウンすると、サーバの起動後に、スケジュール設定されたデバイスのアップロード プロセスが再開されます。IoT FND サーバ クラスタでは、アップロード プロセス時に 1 台のサーバがダウンすると、クラスタ内の別のサーバがプロセスを再開します。

ファームウェア イメージのインストール

ルータ ファームウェア グループ内のデバイスにイメージをインストールするには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、ファームウェア グループを選択します。

   (注)IoT FND は、デバイスをファームウェア固有として認識し、適切なイメージを選択したデバイスにアップロードします。
4. [FIRMWARE IMAGES] ペインで、デバイス サブグループ(IOS-CGR、IOS-WPAN-RF、CDMA など)を選択し、これらのデバイス タイプに表示を調整します。

   上記のステップは、IoT FND がデバイスをファームウェア固有として認識し、システムにより適切なイメージが選択したデバイスに確実にアップロードされるようにするために必要です。
5. [Config] > [Firmware Update] ページで、[Groups] タブをクリックし、[Firmware Upgrade] タブで [Install Image] をクリックします。

   IoT FND はコマンドを送信して、アップロードされたイメージをインストールして機能するようにします。
6. [Yes] をクリックします。

   IoT FND はインストールまたはリロード プロセスを開始します。

(注)イメージのインストール プロセス中に IoT FND を再起動すると、IoT FND は IoT FND がオフラインになる前に実行していたファームウェアのインストール操作を再開します。

次の説明に従って、インストール操作を一時停止または停止することができます。

- ファームウェア イメージのインストールの停止
- FAR ファームウェア イメージのインストールの一時停止と再開
- ファームウェア イメージのインストール、およびその他のアクションからサブネットを除外する

(注)一部のルータでは、ファームウェア インストール操作がタイムアウトになる場合があります。1 時間以上ルータからの応答がない場合、IoT FND はエラー メッセージをログに記録します。

ファームウェア イメージのインストールの停止

ファームウェア イメージのインストールは、いつでも停止できます。イメージのインストールを停止すると、実行中のファームウェア バージョンがそのまま残ります。

(注)インストールを停止すると、キューに入っているすべてのタスクがキャンセルされます。現在実行中のタスクは完了します。

ファームウェア グループ内のデバイスへのファームウェア イメージのインストールを停止するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] をクリックします。
3. [FIRMWARE GROUPS] ペインで、ファームウェア グループを選択します。
4. [Cancel] をクリックします。
5. [Yes] をクリックします。

FAR ファームウェア イメージのインストールの一時停止と再開

ファームウェア イメージのインストール プロセスは、いつでも一時停止できます。

(注)インストール プロセスを一時停止すると、キューに入っているすべてのタスクが一時停止されます。現在実行中のタスクは完了します。

ファームウェア グループ内のデバイスへのファームウェア イメージのインストールを一時停止するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [FIRMWARE GROUPS] ペインで、ファームウェア グループを選択します。
3. [Pause] をクリックします。
4. [Yes] をクリックします。

[Resume] をクリックすると、インストール プロセスを再開できます。

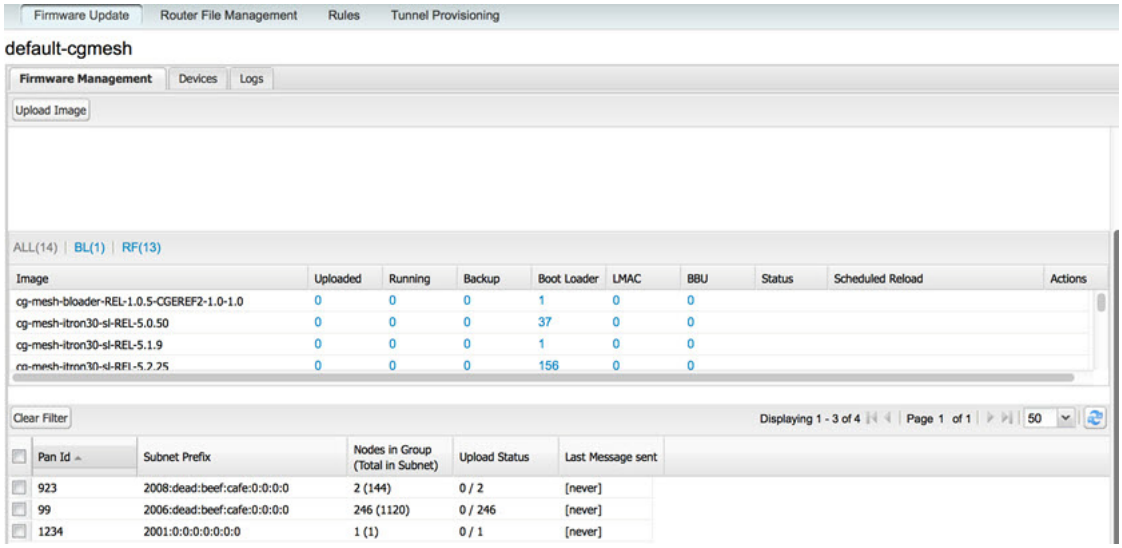
ファームウェア イメージのインストール、およびその他のアクションからサブネットを除外する

[Config] > [Firmware Update] ページ(ページの下部)で、エントリをソート(昇順/降順)できます。

列名にカーソルを合わせて矢印を表示することで、[Pan Id] および [Subnet Prefix] にフィルタを定義できます。これによりアクションを定義し、サブネットの詳細(Pan Id、Subnet Prefix、Nodes in group、Total in subnet、Upload Status、Last Message sent など)を表示できます。

ファームウェア アップグレードのインストールまたはその他のアクションからサブネットを除外するには、そのサブネットの [Pan Id] を選択します。

[Pan Id] のチェック ボックスを選択すると、そのサブネットがファームウェアのアクションから除外されます。



OS の移行

CG-OS から IOS への CGR のアップグレードは、一括でもデバイスごとにでも行えます。移行パッケージは、IoT Field Network Director インストール パッケージ内にあり、[Select IOS Image] メニューで使用できます。

(注) グループ内の CGR がすべて IOS の場合、[Migration to IOS] ボタンは無効化されます。

はじめる前に

CG-OS CGR を移行する場合、デバイス設定プロパティの CSV ファイルまたは XML ファイルに次の IOS プロパティを含めます(デバイス設定プロパティの変更、204 ページを参照)。

ブートストラップ プロパティの例

この例では、移行時にトンネルを維持します。

```
イネーブル化
!
configure terminal
!
!
!
interface GigabitEthernet2/2
    no switchport
    ip address 66.66.0.75 255.255.0.0
    duplex auto
    speed auto
    no shut
!
crypto key generate rsa label LDevID modulus 2048
!
hostname IOS-IOT1
!
enable password cisco
!
aaa new-model
```

```
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
aaa session-id common
clock timezone PDT -8 0
!
!
no ip domain lookup
ip domain name ios.com
ip host nms.sgbu.cisco.com 55.55.0.5
ip host ps.sgbu.cisco.com 55.55.0.8
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!
crypto pki profile enrollment NMS
enrollment url  http://55.55.0.17/certsrv/mscep/mscep.dll
!
crypto pki trustpoint LDevID
    enrollment mode ra
    enrollment profile NMS
    serial-number none
    ip-address none
    password
    fingerprint 1D33B1A88574F11E50F5B758EF217D1D51A7C83F
    subject-name CN=mig.ios.com/serialNumber=PID:CGR1240/K9 SN:JAF1712BCAP
    revocation-check none
    rsakeypair LDevID 2048
!
!
!
license accept end user agreement
license boot module cgr1000 technology-package securityk9
license boot module cgr1000 technology-package datak9
!
!
!
username admin password 0 cisco
username cg-nms-administrator privilege 15 secret Sgbu123!
!
!
do mkdir flash:archive
#await Create directory filename
#send_CR
!
!
archive
    path flash:archive/
    maximum 8
!
!
!
no ip http server
ip http authentication local
ip http secure-server
ip http secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha dhe-aes-256-cbc-sha
ip http secure-client-auth
ip http secure-port 8443
```

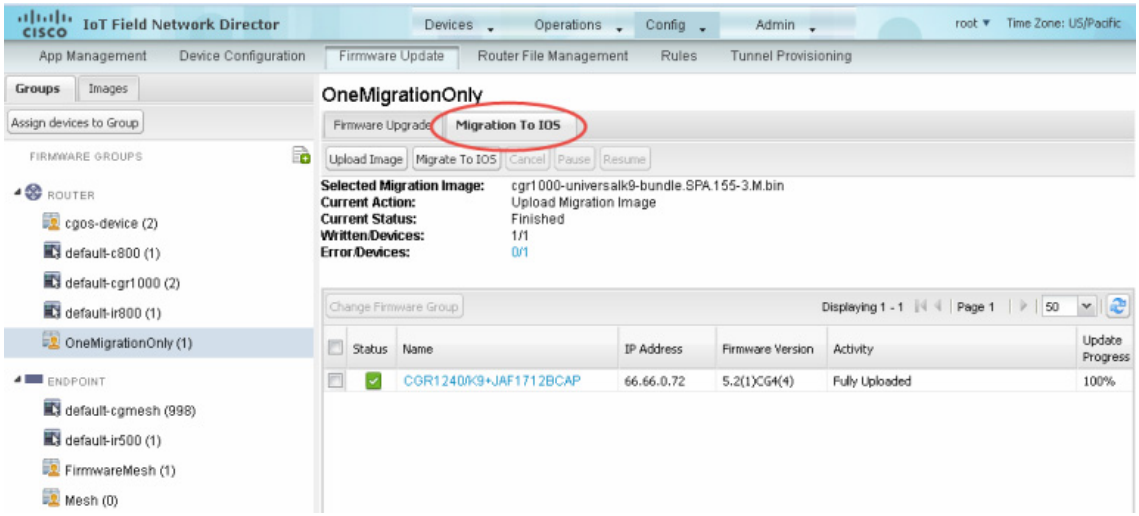
```
ip http secure-trustpoint LDevID
ip http max-connections 2
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client source-interface GigabitEthernet2/2
ip http client secure-ciphersuite aes-128-cbc-sha aes-256-cbc-sha dhe-aes-128-cbc-sha
dhe-aes-256-cbc-sha
!
ip route 0.0.0.0 0.0.0.0 66.66.0.8
!
!
privilege exec level 2 dir /recursive
privilege exec level 2 dir
privilege exec level 2 show memory statistics
privilege exec level 2 show memory
privilege exec level 2 show inventory
privilege exec level 2 show platform hypervisor
privilege exec level 2 show platform led summary
privilege exec level 2 show platform led
privilege exec level 2 show processes cpu
privilege exec level 2 show processes
privilege exec level 2 show environment temperature
privilege exec level 2 show environment
privilege exec level 2 show module
privilege exec level 2 show version
privilege exec level 2 show logging
privilege exec level 2 show platform
privilege exec level 2 show
!
!
wsma agent exec
    profile exec
!
wsma agent config
    profile config
!
!
wsma profile listener exec
    transport https path /wsma/exec
!
wsma profile listener config
    transport https path /wsma/config
!
cgna profile cg-nms-tunnel
    add-command show hosts | format flash:/managed/odm/cg-nms.odm
    add-command show interfaces | format flash:/managed/odm/cg-nms.odm
    add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    add-command show version | format flash:/managed/odm/cg-nms.odm
    interval 10
    url https://ps.sgbu.cisco.com:9120/cgna/ios/tunnel
    active
!
!
cgna exec-profile CGNA-default-exec-profile
    add-command event manager run no_config_replace.tcl flash:/before-tunnel-config cg-nms-tunnel 1 0
    interval 1
    exec-count 1
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager directory user policy "flash:/managed/scripts"
event manager policy tm_ztd_scep.tcl type system authorization bypass
event manager policy no_config_replace.tcl type system authorization bypass
```

```
event manager environment ZTD_SCEP_Enabled TRUE
!
!
do write memory
!
do reload in 005
#await Proceed with reload?
#send_CR
!
crypto pki authenticate LDevID
!
end
```

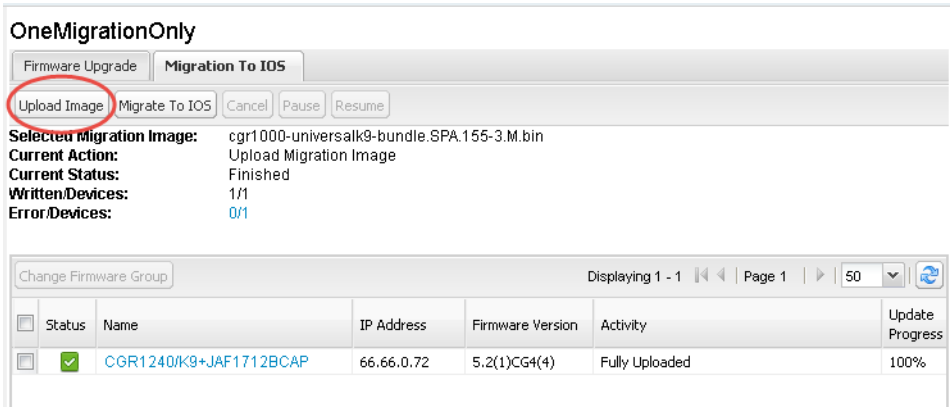
(注) CG4(3) からの移行先は、そのデバイスの最小の IOS イメージに限られます。IOS イメージの最小要件については、表 1 (22 ページ) を参照してください。

CGR IOS イメージを IoT Field Network Director に追加して、移行イメージを CGR にアップロードしてインストールするには、次の手順を実行します。

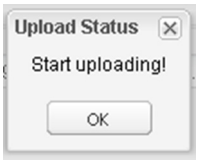
1. [Config] > [Firmware Update] の順に選択し、[Migration to IOS] タブをクリックします。



2. [ROUTERS] ペインで、CGR グループを選択します。
3. グループ移行または個別の CGR のデバイス リストの一番上のチェック ボックスを選択して、[Upload Image] をクリックします。
4. [Select IOS Image] ドロップダウン メニューから、目的のイメージを選択し、[Upload Image] をクリックします。



5. [OK] をクリックしてアップロードを開始します。

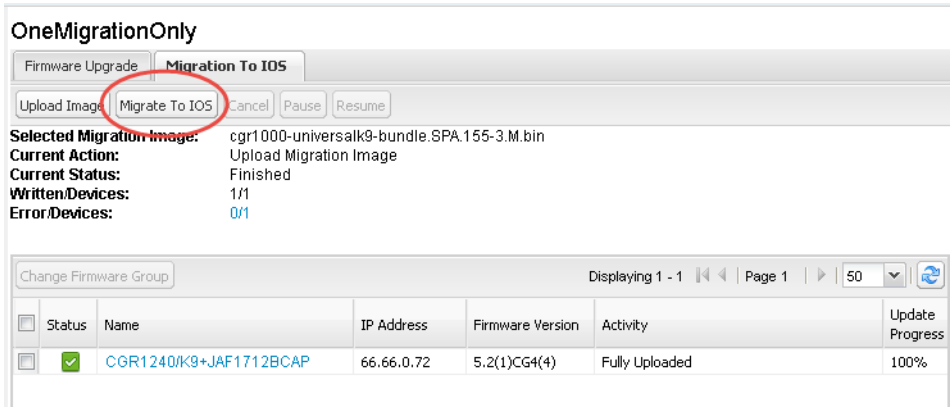


アップロードの進捗がデバイス リストに表示されます。

6. 次のプロパティ ファイルをアップロードします(Cisco IoT FND のインストール、21 ページを参照)。

- config
- ブートストラップ
- トンネル プロビジョニング
- ランタイム設定

7. [Migrate To IOS] ボタンをクリックします。



8. [Yes] をクリックして確定し、移行プロセスを開始します。

デバイス リストで更新の進捗状況を確認できます。エラー メッセージもデバイス リストに表示されます。移行プロセスは、キャンセル、一時停止、または再開することができます。

ヒント:いずれかのルータがアップグレードに失敗した場合、そのグループで移行を再開します。IoT Field Network Director はアップグレード済みのルータをスキップします。

移行後のインターフェイス名

IoT Field Network Director は移行時に、さまざまなインターフェイスのメトリックと関連付けられているプロパティを保存します。表 1 に、CG-OS インターフェイスとメトリックを保存するための対応する IOS インターフェイスのマッピングを示します。

表 1　　CG-OS と IOS インターフェイスの移行マッピング

CG-OS インターフェイス	対応する IOS インターフェイス
Wifi2/1	Dot11Radio2/1
Ethernet2/1	GigabitEthernet2/1
Ethernet2/2	GigabitEthernet2/2
Ethernet2/3	FastEthernet2/3
Ethernet2/4	FastEthernet2/4
Ethernet2/5	FastEthernet2/5
Ethernet2/6	FastEthernet2/6
Wpan4/1	Wpan4/1
Serial1/1	Async1/1
Serial1/2	Async1/2
Cellular3/1	Cellular3/1
該当なし	GigabitEthernet0/1

メッシュ エンドポイント ファームウェア イメージの使用

ここでは、ME ファームウェア イメージを IoT FND に追加する方法と、FAR にイメージをアップロードおよびインストールする方法について説明します。具体的な内容は次のとおりです。

- メッシュ エンドポイント グループへのファームウェア イメージのアップロード
- メッシュ デバイス ファームウェア イメージのアップロード ログの表示
- メッシュ エンドポイント ファームウェア アップデート情報の表示
- ファームウェア イメージのインストール、およびその他のアクションからサブネットを除外する

(注) IR500 とその他のメッシュ エンドポイント デバイスは、ネットワーク上に共存することはできますが、ファームウェア管理では、これらが同じグループに属することはできません。

(注) エンドポイント デバイスは BL/ブート ローダ イメージのタイプを IoT FND に報告できますが、IoT FND はブートローダ イメージをデバイスにアップロードできません。

メッシュ エンドポイント グループへのファームウェア イメージのアップロード

ファームウェア イメージを ME グループ メンバーにアップロードするには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、更新するファームウェア グループを選択します。
4. [Firmware Management] をクリックします。

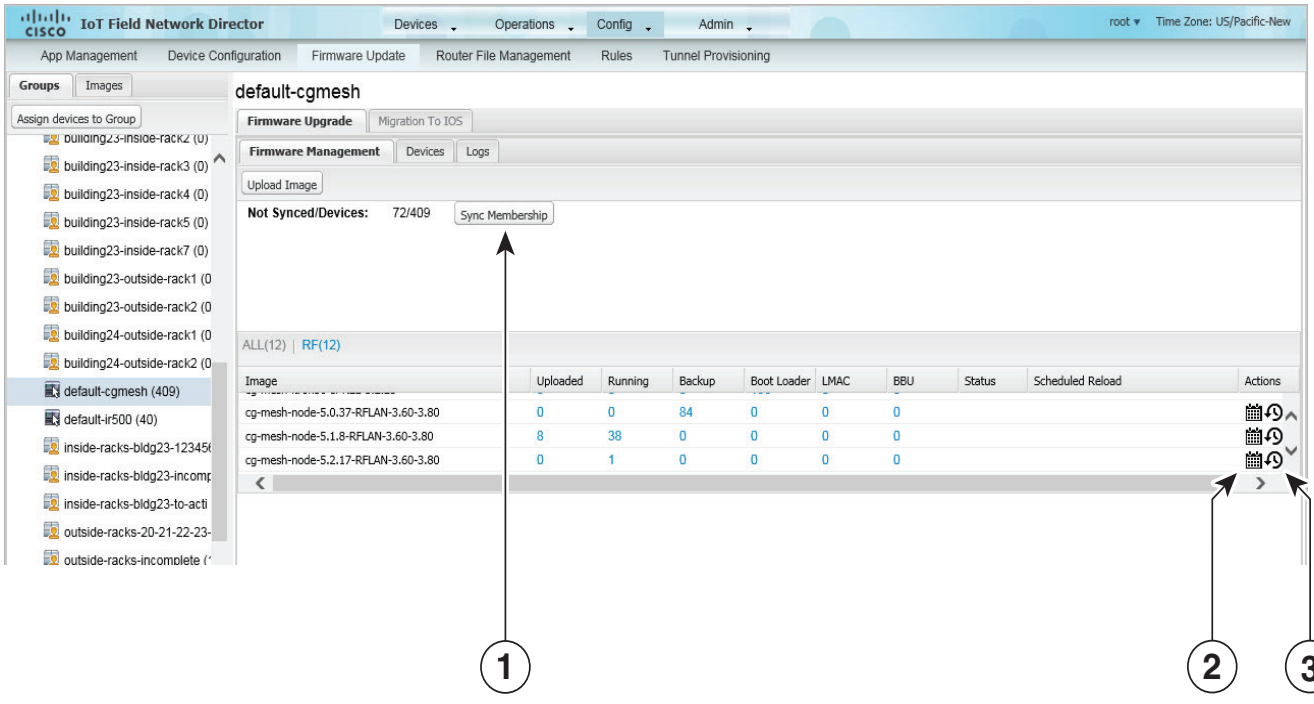
5. [Upload Image] をクリックします。
6. [Select Type:] ドロップダウン メニューから、使用中のデバイスのファームウェア タイプを選択します。

   IoT FND では、これらのイメージ タイプを ENDPOINT デバイスにアップロードできます。

Image Type	説明
RF	RFLAN が接続されているデバイス。
PLC	電力線通信デバイス。
BBU	バッテリ バックアップがあるデバイス。
LMAC	ローカル MAC が接続されているデバイス。
PLC-RF	PLC 無線周波数デバイス。

7. [Select an Image:] ドロップダウン メニューから、アップロードするファームウェア バンドルを選択します。
8. [Upload Image] をクリックします。
9. [OK] をクリックします。

   IoT FND はイメージを [Firmware Management] ペインのイメージ リストに追加し、バックグラウンドでアップロード プロセスを開始します。



1 [Sync membership] ボタン
2 [Schedule Install and Reload] ボタン
3 [Set as Backup] ボタン

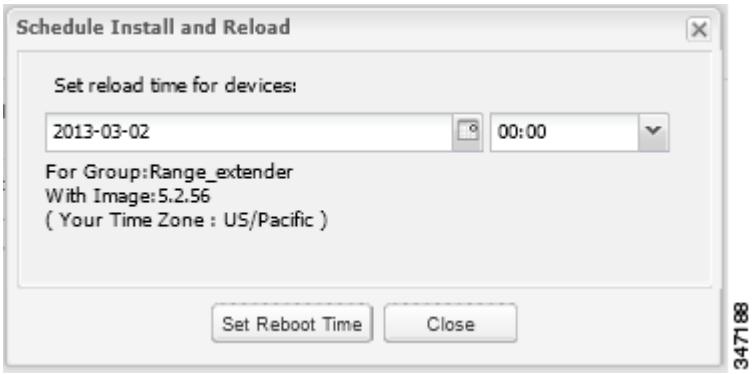
リスト内のすべてのイメージに対し、IoT FND は次の情報を表示します。

カラム	説明
Image	イメージ名。
Uploaded	イメージをアップロードしたデバイスの数を指定します。数値をクリックすると、これらのデバイスのリストが表示されます。
Running	このイメージを実行しているデバイスの数を指定します。数値をクリックすると、これらのデバイスのリストが表示されます。
バックアップ	このイメージをバックアップとして使用しているデバイスの数を指定します。数値をクリックすると、これらのデバイスのリストが表示されます。
ブート ローダ	ブート ローダ イメージのバージョンを指定します。
LMAC	LMAC イメージのバージョンを指定します。
BBU	BBU イメージのバージョンを指定します。
Status（ステータス）	アップロード プロセスのステータスを指定します。
Scheduled Reload	スケジュール設定されたリロード時間を指定します。
Actions	次の 2 つのアクションを提供します。 ■ Schedule Install and Reload：ロードされたイメージのインストールと、ME の再起動をスケジュール設定します。 ■ Set as Backup：イメージをバックアップ イメージとして設定します。

インストール スケジュールの設定

インストール スケジュールを設定するには、次の手順を実行します。

1. [Schedule Install and Reload] ボタン（2）をクリックします。
2. イメージのインストールとデバイスを再起動する日時を指定します。



3. [Set Reboot Time] をクリックします。
   - 選択したイメージをファームウェア イメージ バックアップとして設定するには、[Set as Backup] ボタン（3）をクリックします。

4. [Yes] をクリックします。

- 同じファームウェア グループ内のグループ メンバーを同期するには、[Sync Membership](1)をクリックします。
- メンバーのデバイスを表示するには、[Devices] タブをクリックします。
- グループのログ ファイルを表示するには、[Logs] タブをクリックします。

メッシュ デバイス ファームウェア イメージのアップロード ログの表示

メッシュ デバイスのファームウェア イメージのアップロード ログを表示するには、次の手順を実行します。

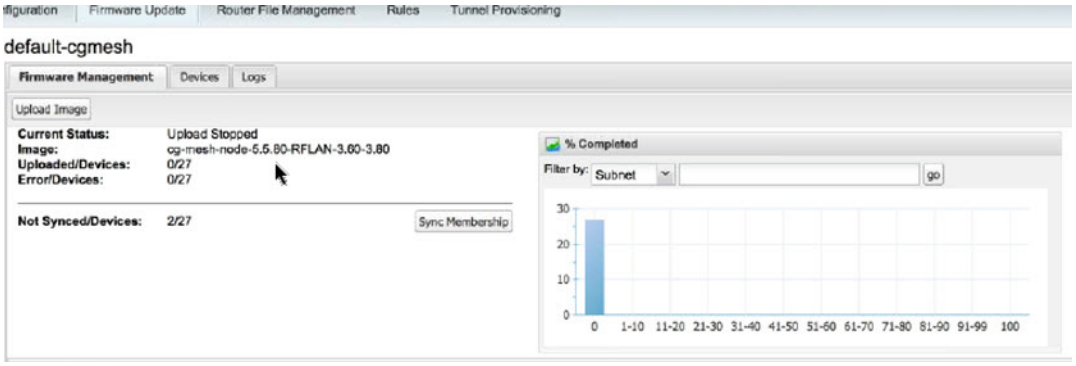
1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、メッシュ デバイス ファームウェア グループを選択します。
4. [Logs] タブをクリックします。

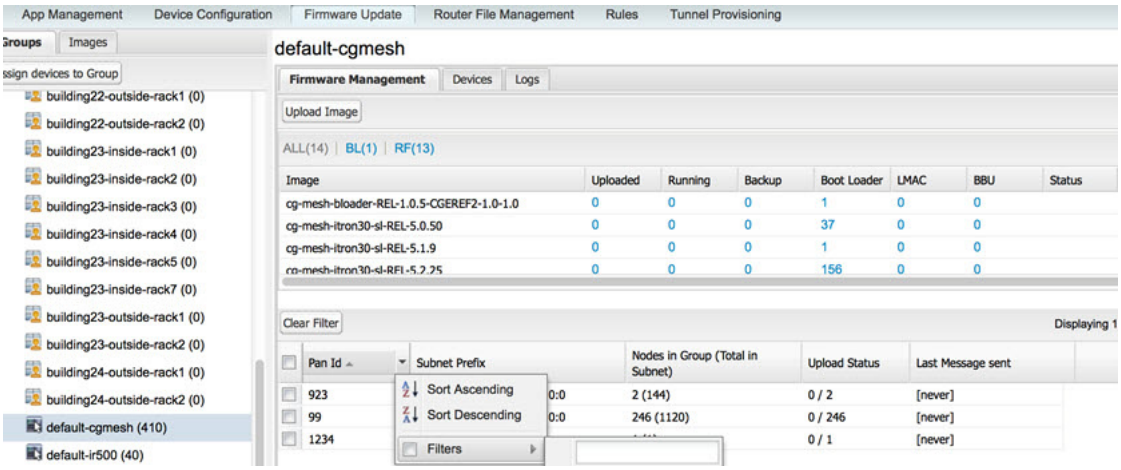
メッシュ エンドポイント ファームウェア アップデート情報の表示

より見やすくするため、エンドポイント ファームウェア アップデート プロセスからサブネット レベルまでを表示できます。アップグレード プロセス中、またはファームウェアのアップグレードが完了した後に、メッシュ エンドポイント デバイスのファームウェア アップデートの詳細(Subnet、Pan ID または Group ごと)を表またはヒストグラムで表示するには、以下のステップに従います。

(注) Subnet および Pan ID の場合、表示されているテキスト ボックスに値を入力する必要があります。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、MESH DEVICES グループを選択します。
4. [Firmware Management] タブをクリックします。





フィールド	説明
(左上のパネル)	
[Upload Image] ラジオ ボタン	ラジオ ボタンをクリックすると、ファームウェアのアップロードが開始されます。(注)デフォルトでは、画面の下部にリストされているすべてのサブネットがイメージのアップロードを受け取ります。 ファームウェアのアップロードから**サブネットを除外する**には、除外するサブネットの横のチェック ボックス(1 または 2 など)をオンにします。詳細については、後述する PAN ID 定義を参照してください。
Current Status	ファームウェア アップロードのステータス(「Image Loading」や「Upload Finished」など)。 ■ Image Loading、Upload Paused、Upload Stopped、Upload Finished、Upload Stopping、Upload Pausing ■ Scheduling Reload、Reload Paused、Reload Stopped、Reload Scheduling Finished、Reload Stopping、Reload Pausing ■ Setting Backup、Backup Paused、Backup Stopped、Backup Finished、Backup Stopping、Backup Pausing
Image	ファームウェア イメージ名。
Uploaded/Devices	アップデートを受け取るデバイスの総数に対し、ファームウェアのアップデートが正常に完了した数。
Error/Devices	グループ内のデバイスの総数に対し、操作が失敗(エラー)したデバイスの数。
Not Synced/Devices	グループ内のデバイスの総数に対し、ファームウェア グループ メンバーシップの同期されていないデバイスの数。
(右側のパネル)ヒストグラム	
% Completed	アップロードの進捗度(パーセンテージ)の視覚ステータス。
Filter by	[Subnet]、[Pan ID]、[Group] ごとに結果をフィルタ処理して表示します。

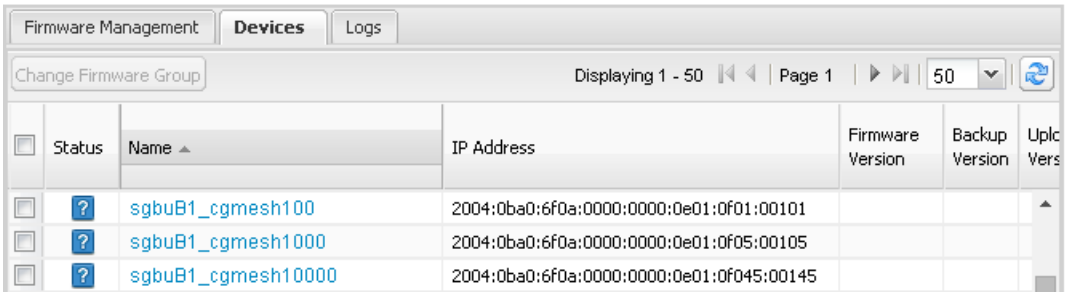
フィールド	説明
（下のパネル）	
All または RF	[All] では、[Running]、[Uploaded]、[Backup] のスロット内のすべてのイメージに関する情報に加え、グループ内のすべてのデバイス イメージの BBU および PLC 情報（RF メッシュ、BBU および PLC がある IR500 WPAN Range Extender および WPAN Range Extender）、およびリロードのスケジュールとステータス情報が表示されます。 [RF] では、[Running]、[Uploaded]、[Backup] のスロット内の RF メッシュ イメージに関する情報と、リロードのスケジュールとステータス情報が表示されます。
Image	イメージ ファイル名が表示され、次のステータスに関するファームウェアのアップロードの進捗度のパーセンテージ（0 ～ 100）が提供されます。 ■ Uploaded、Running、Backup、Bootloader、LMAC、BBU、Status、Sched Reload
Clear filter	ラジオ ボタンをクリックすると、選択したファームウェア イメージの更新結果がクリアされます。
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。 新しいファームウェアのアップロードからノードのグループを**除外**するには、そのノードのグループの横にある [Pan ID] チェック ボックスを選択してから、[Firmware Management] ペインの [Upload Image] ラジオ ボタンを選択する必要があります。 (注) PAN ID の横のチェック ボックスは、ファームウェアのアップロード中には表示されません。 (注) PAN ID を昇順または降順にソートしたり、PAN ID でフィルタ処理してウィンドウに表示する PAN ID を定義することができます。これには列の右側にある下向き矢印を選択します。そのビューから戻るには、[Clear Filter] を選択します。 (注) サブネット内のすべてのノードのリストを表示するには、[Devices] タブを選択します。
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。特定のサブネット内のノードをすべて表示するには、[Devices] タブを選択します。 (注) 列の右側の下向き矢印を選択して、サブネットの一部（200b:0:0 など）を入力して、サブネットでフィルタリングできます。そのビューから戻るには、[Clear Filter] を選択します。
Nodes in Group	グループ内のノードの数。上記のスクリーン ショットでは、グループ内に合計 25 ノードあり、これらが 2 つの異なるサブネットに分割されています（200b:0:0:0:0:0:0:0 に 8 ノード、200c:0:0:0:0:0:0:0 に 17 ノード）。
Total in Subnet	サブネット内のノードの数。上記のスクリーン ショットでは、サブネットに 19 のノードがあります。
Upload status	合計ノードのうち、新しいファームウェアで正常にアップグレードされたノードの数。
Last message sent	特定の PAN 内の現在のファームウェア アップデート プロセスに関連する最新のメッセージが表示されます。

メッシュ デバイスのファームウェア情報の表示

メッシュ デバイスのファームウェア情報を表示するには、次の手順を実行します。

1. [Config] > [Firmware Update] の順に選択します。
2. [Groups] タブをクリックします。
3. [FIRMWARE GROUPS] ペインで、MESH DEVICES グループを選択します。

4. [Devices] タブをクリックします。



IoT FND はグループ内のすべてのデバイスに対してこの情報を表示します。

フィールド	説明
Status（ステータス）	デバイスのステータス（Up、Down、Unheard など）。
名前	デバイスの EID。
IP アドレス	デバイスの IP アドレス。
Firmware Version	デバイスで実行されているファームウェア イメージのバージョン。
バックアップ バージョン	バックアップとして使用されているファームウェア イメージのバージョン。
Uploaded Version	デバイスにロードされているファームウェア イメージのバージョン。
Member Synced?	デバイスがグループ内の他のデバイスと同期しているかどうか。
アクティブな状態	ファームウェア イメージのアップロード アクティビティ。
Update Progress	ファームウェア イメージのアップロードの進捗。アップロードの進捗が 100% になると、アップロードが完了したことを示します。
Last Firmware Status Heard	最後に確認されたファームウェア ステータス。
Scheduled Reload Time	アップロード イメージのリロードの時刻設定。
エラー メッセージ	イメージのアップロードに失敗した場合のエラー メッセージ。

トンネルのプロビジョニングの管理

ここでは、IoT FND を設定してトンネルのプロビジョニングを行う方法、および FAR（CGR と C800）および HER を接続するトンネルを管理およびモニタする方法について説明します。具体的な内容は、次のとおりです。

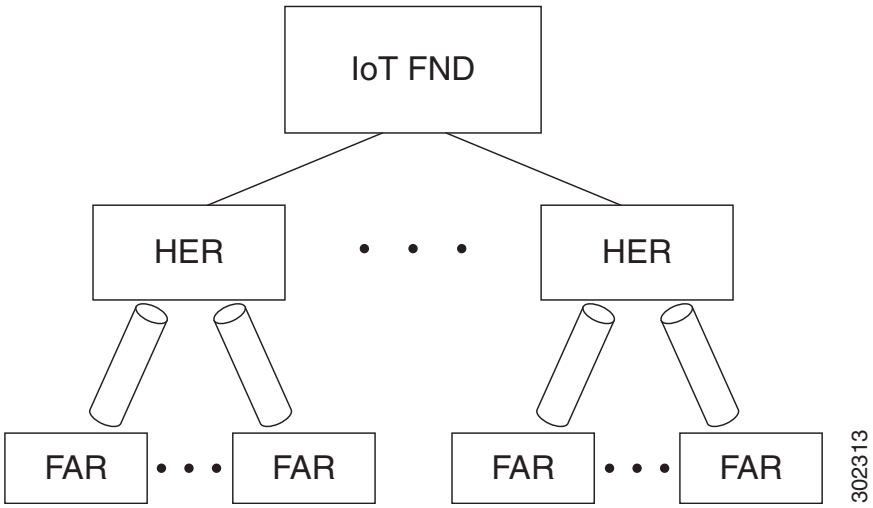
概要

IoT FND は、トンネルのプロビジョニング テンプレートを処理することにより生成されたコマンドを FAR および HER に送信し、その間に安全なトンネルをプロビジョニングします。デフォルトの IoT FND テンプレートには CLI コマンドが含まれ、GRE および IPsec トンネルをセットアップおよび構成します。1 つの HER で、同じ HER EID および名前を持つ複数のトンネルを含む、500 までの FAR を実行できます。

（注）IoT FND リリース 3.1.x を使用して始める場合、ネットワークへの FAR の導入前に、FAR と HER の間に IPSec トンネルのプロビジョニングを設定する必要がなくなります（図 1に示します）。

代わりに、トンネル プロビジョニング テンプレートに CLI が含まれないようにして設定する、**IPSec なしの ZTD** を開始できます。工場出荷時の設定*なし*にネットワークを起動するこの最初のアプローチは、ネットワークにおけるこの後の IPSec 使用を排除するものではありません。

図 1　　トンネルは、FAR とそれに対応する HER を接続します



HER および FAR の間にトンネルをプロビジョニングするため、IoT FND はこれらのデバイスで CLI トンネル設定コマンドを実行します。デフォルトでは、IoT FND は CLI トンネル設定コマンドを含む基本的なトンネル設定テンプレートを提供します。また、お使いのテンプレートを使用することもできます。トンネルのプロビジョニング プロセスは自動ですが、最初に トンネル プロビジョニング設定プロセス に概要が示されている設定手順を実行する必要があります。この後、FAR がオンライ

ンになると必ず、IoT FND により自動的にトンネルでプロビジョニングされます。IoT FND をトンネルのプロビジョニング用に設定する前に、IoT FND TPS プロキシがインストールおよび実行されていることを確認します。

トンネル プロビジョニング設定プロセス

トンネルのプロビジョニングを設定する前に、IoT FND 上にキーストア ファイルおよび TPS プロキシを生成する必要があります。次に、相互に通話するようIoT FNDおよび TPS プロキシを設定します（TPS プロキシの設定およびTPS プロキシを使用するための IoT FND の設定）

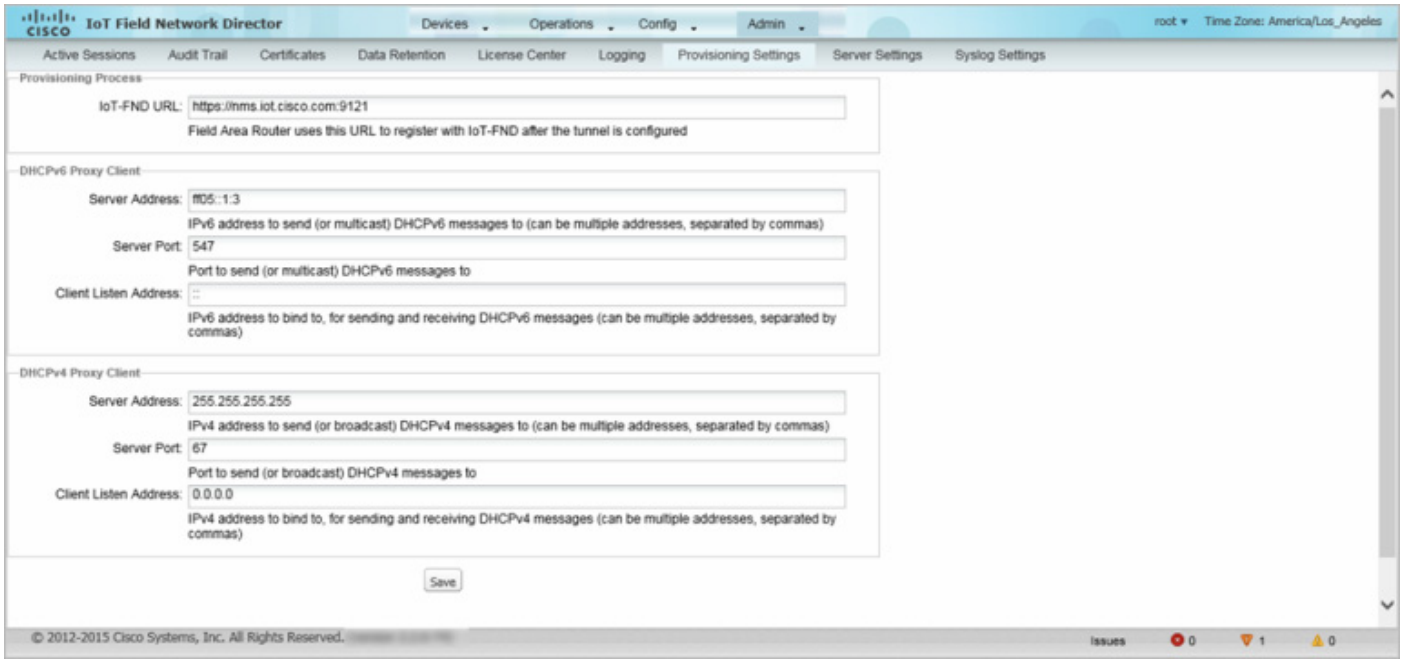
IoT FND を設定してトンネル プロビジョニングを行うには、次の手順を実行します。

		備考
1.	（CG-OS CGR）DHCP サーバを設定します。 DHCP サーバを設定して IoT FND に一意の IP アドレスを提供します。デフォルトの IoT FND トンネル プロビジョニング テンプレートにより、トンネルを作成するために必要なループバック インターフェイスと IP アドレスが設定されます。 Cisco IOS CGR は FlexVPN を使用します。テンプレートに含まれるのがループバック インターフェイスのアドレスのみであることを確認します。	DHCP サーバーにトンネル プロビジョニングを設定。
2.	トンネル設定を行います。 IoT FND のプロビジョニング設定ページで NMS URL と DHCP プロキシ クライアントの設定を行います（[Admin] > [System Management] >[Provisioning Settings]）。	プロビジョニングの設定。
3.	（CG-OS CGR）FAR 登録要求を最初のコンタクト（*call home*）で受け入れるように IoT FND を設定してトンネルのプロビジョニングを要求します。 Cisco IOS CGR は CGNA サービスを利用します。	
4.	HER 管理を設定します。 SSH で NETCONF を使用した IoT FND による管理を行うため HER を設定します。	IoT FND への追加前の HER の設定。
5.	HER を IoT FND に追加します。	IoT FND への HER の追加。
6.	IoT FND トンネル プロビジョニング テンプレートを確認して、正しいタイプのトンネルを作成していることを確認します。	
7.	（任意）トンネルのプロビジョニングに独自のテンプレートを使用する場合、1 つ以上のトンネルプロビジョニング グループを作成して、デフォルトのトンネル プロビジョニング テンプレートを変更します。	トンネル プロビジョニング テンプレートの設定。
8.	（CG-OS CGR）Call Home を発信するため FAR を設定します。 FAR がIoT FND TPS プロキシを通じて HTTPS で IoT FND に連絡するように設定します。	この手順は通常、FAR が TPS プロキシに連絡するよう設定されている工場で実行されます。
9.	FAR を IoT FND に追加します。 出荷通知 XML ファイルを使用して FAR を IoT FND にインポートします。	IoT FND への FAR の追加。
10.	FAR を対応する HER にマッピングします。	FAR の HER へのマッピング。

以上の手順を完了した後、FAR を展開し、電源を入れます。トンネルのプロビジョニングが自動的に行われます。

以下は、FAR をオンにした後のイベントのシーケンスです。

1. FAR がオンになり、アップリンク ネットワークに接続すると、証明書の登録のリクエストを送信します。
2. その後、IoT FND TPS プロキシによって IoT FND にトンネルのプロビジョニングを要求します。
3. IoT FND は IoT FND データベースの FAR レコードを調べ、使用するトンネル プロビジョニング テンプレートを決定します。IoT FND は、トンネルを確立するため HER の経路を調べます。
4. Cisco IOS CGR では、デフォルトのテンプレートは FlexVPN を使用するよう CGR を設定します。FlexVPN クライアントが CGR に設定され、CGR は HER に連絡して FlexVPN トンネルが動的に構築されるよう要求します。以上が、HER が CGR の新しいトンネル エンドポイント インターフェイスを動的に追加する方法です。
5. FAR のテンプレートを処理する前に、IoT FND は HER トンネル削除テンプレートを処理し、その結果であるコマンドを HER に送信します。これは、各 HER に対して行われ、FAR に関連付けられている可能性がある既存のトンネル設定を削除します。
6. IoT FND は FreeMarker テンプレート エンジンを使用して、FAR トンネル追加テンプレートを処理します。エンジンはテンプレートを IoT FND により CLI 設定コマンドと仮定されるテキストに変換します（CGR ごとに CG-OS または Cisco IOS）。IoT FND はこれらのコマンドを使用して、FAR にトンネルの一端を設定し、立ち上げます。
7. IoT FND は FreeMarker テンプレート エンジンを使用して、HER トンネル追加テンプレートを処理します。エンジンはテンプレートを、IoT FND により HER のトンネル設定のためのコマンドと仮定されるテキストに変換します。
8. この手順は OS に固有のものです。
   - Cisco IOS CGR では、テンプレートにより生成されたコマンドを FAR と HER に適用してエラーが起きなければ、IoT FND は新しくアクティブな CGNA プロファイル「cg-nms-register」を設定し、「cg-nms-tunnel」プロファイルを無効にします。Cg-nms-register プロファイルは、IoT FND URL を使用します。
   - CG-OS CGR では、IoT FND は Call Home URL をプロビジョニング設定ページ（[Admin] > [System Management] > [Provisioning Settings]）で指定される IoT FND URL に再設定します。



指定された URL は、トンネル プロビジョニング ポートの代わりに IoT FND の登録ポート（デフォルトで 9121）を使用します。この URL の 完全修飾ドメイン名（FQDN）は異なっており、トンネル経由でのみ到達可能な IP アドレスに解決します。

トンネル プロビジョニングの設定

ここでは、トンネル プロビジョニング用に IoT FND を設定する方法について説明します。

- DHCP サーバーにトンネル プロビジョニングを設定
- CNR を使用したトンネルのプロビジョニング用 DHCP 設定

DHCP サーバーにトンネル プロビジョニングを設定

トンネルのプロビジョニングを成功させるには、IoT FND によって使用される DHCP サーバーを設定し、アドレスを指定して FAR と HER の間にトンネルを作ります。たとえば、パーマネント リースの原則に基づき、DHCP サーバを設定して、トンネルのプロビジョニングに IP アドレスを提供します。

IoT FND はトンネル プロビジョニング テンプレートで定義された設定に基づいて DHCP 要求を行います。トンネルのプロビジョニングの間、IoT FND テンプレートは 2 種類の DHCP 要求を行うことができます。

- IP アドレスを要求した後、テンプレートで使用可能にします。
- 2 つの IP アドレスのサブネットを要求し、両方のアドレスをテンプレートで使用可能にします。

IoT FND は これらの要求を IPv4 アドレス、IPv6 アドレス用に行うことができます。

テンプレートから DHCP アドレスを要求する機能は、トンネルの設定を定義する際の柔軟性を最大に高めます。各 FAR および対応する HER のインターフェイスに必要な正確なアドレスを割り当てるためです。提供されるデフォルトのトンネル プロビジョニング テンプレートは、最も一般的な使用法の例、FAR とそれに対応する HER の間の 1 つの IPsec トンネルを定義します。この IPsec トンネルの両端が、動的に割り当てられた IPv4 アドレスを取得します。

- ご使用の DHCP サーバがサブネットの割り当てをサポートしている場合、同じサブネットに属する 2 つのアドレスを取得するためにこれを使用します。
- ご使用の DHCP サーバが、アドレスの割り当てのみをサポートしている場合、2 つの DHCP アドレスが IPsec トンネルの両端として使用できるリターン アドレスを要求するように設定します。
- ルーティング プランが、各 FAR に一意の IPv4 アドレスを割り当て、それを、IPsec トンネル上のループバック インターフェイスに割り当てる必要がある場合、IoT FND テンプレートを使用してこのアドレスを割り当てます。

IPv6 GRE トンネルを作成することを選択する場合、DHCP プレフィックス委任または個々のアドレス要求を使用して、トンネルの両端に IPv6 アドレスを割り当てます。

ここでは、トンネルのプロビジョニングの DHCP 設定例について説明します。これらの設定の設定方法は、ご使用の装置によって異なります。この項では、Cisco Network Registrar（CNR）を使用してトンネルのプロビジョニング向けに DHCP サーバを設定するための一般的な注意事項を説明します。

CNR を使用したトンネルのプロビジョニング用 DHCP 設定

次にあげる CNR の CLI スクリプト例は、IoT FND のデフォルトのトンネル プロビジョニング テンプレートから発信したリクエストを処理するよう、CNR DHCP サーバを設定します。このスクリプトを使用する際は、サブネットがご使用の DHCP サーバ環境に適していることを確認してください。

CNR DHCP サーバ のトンネル プロビジョニング スクリプト例

```
# These commented out commands support re-applying the configuration by first
# removing any previously applied configuration, in reverse order.This should
# not be done in a production environment, but may be useful when initially
# developing and testing a configuration.

# scope v4address-perm delete
# dhcp-address-block v4subnet-perm delete
# prefix v6subnet-perm delete
# prefix v6address-perm delete
```

```
# policy permanent delete

# Configure the server to automatically map any IPv4 or IPv6 user class
# option values to selection tags.By default CG-NMS includes a value of
# "CG-NMS" for the user class in its requests.The tag is used to insure
# prefixes and scopes configured to satisfy requests from CG-NMS are only
# used for that purpose.

dhcp set map-user-class-id=append-to-tags

# Since CG-NMS uses the leased addresses and subnets in router
# configuration the addresses and subnets must be permanently allocated
# for that purpose.Create a policy that instructs the DHCP server to
# offer a permanent lease.

policy permanent create
policy permanent set permanent-leases=enabled

# Configure DHCPv6.

# The default CG-NMS tunnel template will request IPv6 addresses for
# use with CGR loopback interfaces.

prefix v6address-perm create 2001:DB8:0:0:1::/80 dhcp-type=dhcp
prefix v6address-perm set description="Pool for leasing addresses for loopback interfaces."
prefix v6address-perm set policy=permanent
prefix v6address-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv6 prefixes for
# use with GRE tunnels.Force use of a /127 prefix.

prefix v6subnet-perm create 2001:DB8:0:0:2::/80 dhcp-type=prefix-delegation
prefix v6subnet-perm set description="Pool for leasing prefixes for GRE tunnels."
prefix v6subnet-perm set policy=permanent
prefix v6subnet-perm set selection-tags=CG-NMS
prefix-policy v6subnet-perm set default-prefix-length=127
prefix-policy v6subnet-perm set shortest-prefix-length=127

# Configure DHCPv4.

# The default CG-NMS tunnel template will request IPv4 subnets for
# use with IPsec tunnels.Note that currently address pools for
# IPv4 subnet allocation can only be configured using the CLI as the
# CNR Web UI does not currently support them.

# If CNR allowed you to set a description on DHCP address blocks it would be:
# "Pool for leasing subnets for IPsec tunnels."

dhcp-address-block v4subnet-perm create 192.0.2.0/24
dhcp-address-block v4subnet-perm set default-subnet-size=31
dhcp-address-block v4subnet-perm set policy=permanent
dhcp-address-block v4subnet-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv4 addresses for
# use with loopback interfaces.

scope v4address-perm create 198.51.100.0 255.255.255.0
scope v4address-perm set description="Pool for leasing addresses for loopback interfaces."
scope v4address-perm set policy=permanent
scope v4address-perm addRange 198.51.100.2 198.51.100.254
scope v4address-perm set selection-tag-list=CG-NMS

# Configure detailed logging of incoming and outgoing packets.This is useful when
```

```
# debugging issues involving DHCP, however this level of logging will lower the
# performance of the DHCP server.this is a production server under heavy load
# it may be necessary to forgo detailed packet logging.

dhcp set
log-settings=missing-options,incoming-packet-detail,outgoing-packet-detail,unknown-criteria,client-deta
il,client-criteria-processing,dropped-waiting-packets,v6-lease-detail

# Save the changes and reload the server to have them take effect.
save
dhcp reload

# List the current configuration.

policy list
プレフィックス リスト
dhcp-address-block list
scope list
dhcp show
```

トンネル グループ 設定の構成

FAR のトンネル プロビジョニングを一括で設定するには、IoT FND でグループを使用します。デフォルトでは、IoT FND に追加されたすべての FAR（デバイスの一括追加 を参照）は、適切なデフォルト グループ **default-cgr1000** または **default-c800** です。デフォルト グループには、IoT FND がトンネルのプロビジョニングに使用する 3 つのテンプレートが含まれています。

ここでは、次の内容を説明します。

- トンネル グループの作成
- トンネル グループの削除
- トンネル グループの表示
- FAR の別のグループへの移動
- トンネル グループの名前の変更

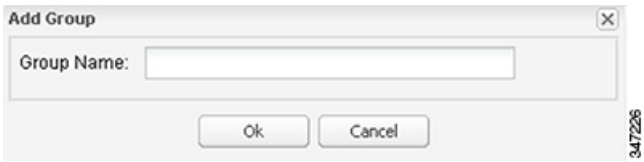
トンネル グループの作成

すべての FAR に 1 組のテンプレートの使用を予定している場合、使用するのがデフォルトのテンプレート、修正されたデフォルトのテンプレート、またはカスタム テンプレートのいずれであっても、追加のグループは作成しないでください。複数組のテンプレートを定義するには、グループを作成し、それらのグループのテンプレートをカスタマイズします。

（注） ご使用のカスタム テンプレートが両方のルータのタイプに適用可能な場合、CGR と C800 を同じトンネル プロビジョニング グループに入れることができます。

トンネル グループを作成する方法：

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [Add Group]（ ）をクリックします。



3. 新しいグループの名前を入力し、[OK] をクリックします。

   グループが [TUNNEL GROUPS] ペインに表示されます。

トンネル グループを作成した後、FAR の別のグループへの移動に示すように、他のグループから FAR を移動します。

トンネル グループの削除

空白のグループのみが削除できます。トンネル グループを削除するには、そこに含まれているデバイスを他のグループに移動する必要があります。

空白のトンネル グループを削除する方法:

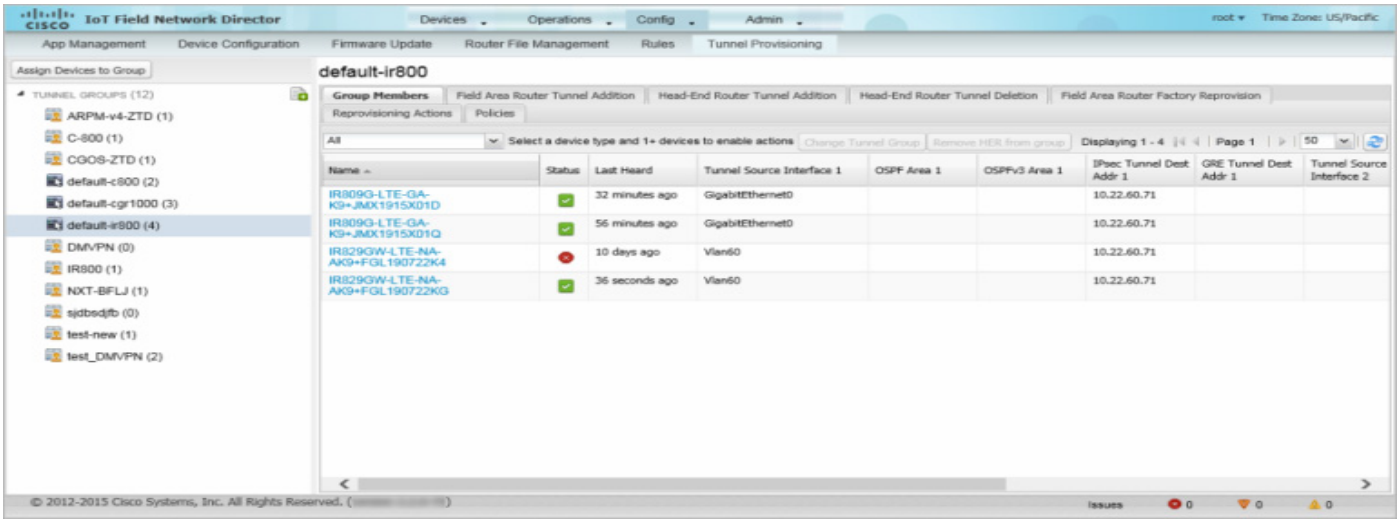
1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、削除するトンネル グループを選択します。
3. [Delete Group](−)をクリックします。
4. [Yes] をクリックします。

トンネル グループの表示

トンネルのプロビジョニング ページでは、既存のトンネル グループに関する情報を一覧表示します。

IoT FND に定義されたトンネル グループを表示するには、次の手順を実行します。

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [Group Members] をクリックします。
3. [TUNNEL GROUPS] ペインで、グループを選択します。



IoT FND によりグループ内のすべての FAR のリストが表示されます。リスト ナビゲーション ボタンを使用してリストをスクロールします。表 1 に、リスト フィールドを示します。

表 1　　トンネル グループ フィールド

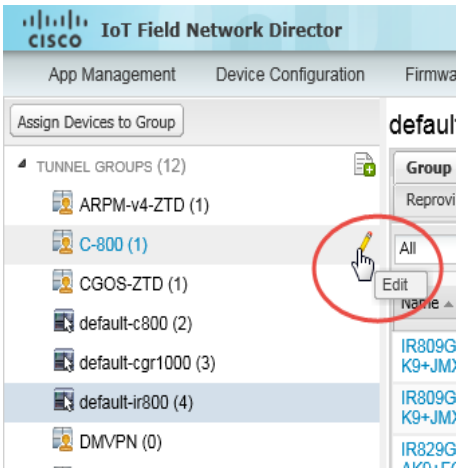
フィールド	説明
名前	FAR EID（デバイス ID）
Status（ステータス）	FAR のステータス： ■ Unheard：FAR はまだ IoT FND を接続していません。 ■ Unsupported：FAR は IoT FND によってサポートされていません。 (注) CGR 1000 シリーズ ルータのみがサポートされています。 ■ Up：FAR は稼働しています。 ■ Down：FAR はオフになっています。
Last Heard	ルータが IoT FND に最後にコンタクトした、またはメトリックを送信した時間。ルータが IoT FND にコンタクトしていなければ、このフィールドに **never** が表示されます。そうでない場合、IoT FND は最後のコンタクトの日時、たとえば **4/10 19:06** を表示します。
Tunnel Source Interface 1 Tunnel Source Interface 2	トンネルで使用されている FAR インターフェイス。
OSPF Area 1 OSPF Area 2	Open Shortest Path First（OSPF）のエリア 1 および 2。
OSPFv3 Area 1	OSPFv3 のエリア 1。
IPsec Dest Addr 1 IPsec Dest Addr 2	トンネルの IPv4 宛先アドレス。
GRE Tunnel Dest Addr 1 GRE Tunnel Dest Addr 2	IPv6 宛先アドレス。
Certificate Issuer Common Name	証明書を発行した CA の名前。

トンネル グループの名前の変更

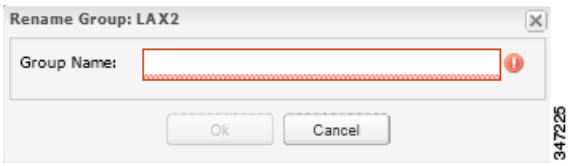
トンネル グループの名前はいつでも変更できます。シスコでは、短くわかりやすい名前を使用することをお勧めしています。名前は 250 文字以内である必要があります。

トンネル グループの名前を変更する方法：

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、名前を変更するトンネル グループをロールオーバーして、[Edit] の鉛筆のアイコン（ ）をクリックします。



3. 新しい名前を入力して [OK] をクリックします。



(注) 上に示すとおり、無効な文字(@、#、!、+など)をフィールドに入力すると、フィールドが赤くハイライトされて [OK] ボタンが無効化されます。

FAR の別のグループへの移動

FAR を別のグループに移動するには、次の 2 つの方法があります。

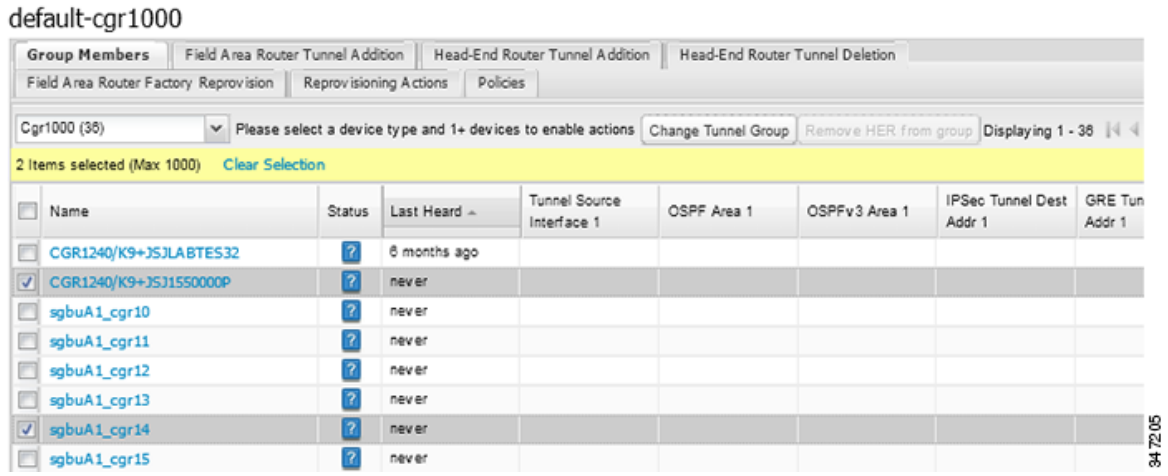
- FAR を手動で別のグループに移動
- FAR を一括で別のグループに移動

FAR を手動で別のグループに移動

FAR を手動で別のグループに移動する方法:

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [Group Members] タブをクリックします。
3. [TUNNEL GROUPS] ペインで、移動するトンネル グループとルータを選択します。
4. [Select a device type] ドロップダウン メニューから、デバイスのタイプを選択します。
5. 移動する FAR のチェック ボックスにチェックを入れます。

   グループ内のすべての FAR を選択するには、カラムの一番上にあるチェック ボックスをクリックします。デバイスを選択すると、選択されたデバイスの数を表示し、[Clear Selection] と [Select All] のコマンドがある黄色いバーが表示されます。選択できるデバイスの最大数は 1000 です。
6. [Change Tunnel Group] ボタンをクリックします。



7. ドロップダウン メニューから、FAR の移動先のトンネル グループを選択します。

8. [Change Tunnel Group] をクリックします。
9. [OK] をクリックして、ダイアログボックスを閉じます。

FAR を一括で別のグループに移動

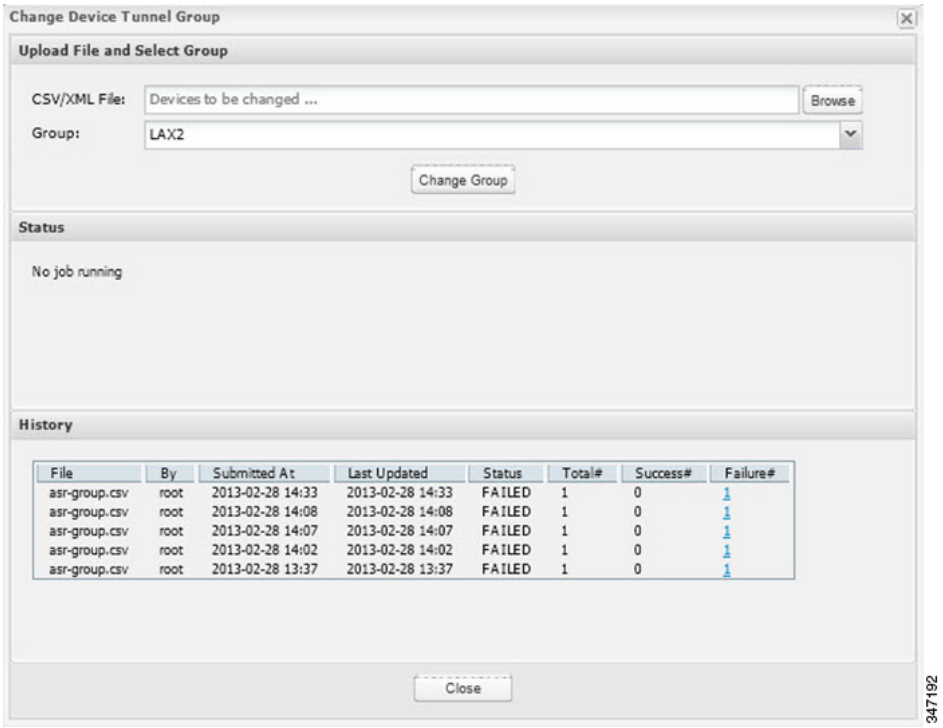
移動する FAR の名前を含む CSV または XML ファイルをインポートすることで、FAR を一括で別のグループに移動できます。エントリが、次にあげるフォーマットでファイルに含まれていることを確認してください。

```
eid
CGR1120/k9+JSM1
CGR1120/k9+JSM2
CGR1120/k9+JSM3
CGR1120/k9+JSM4
C819HGW-S-A-K9+FTX174685V0
```

最初の行はヘッダーで、残りの行に FAR EID が入ることを IoT FND に 伝えます（1 行あたり FAR EID 1 つ）。

FAR を一括で別のグループに移動する方法：

1. 異なるグループに移動するデバイスの EID を 含む CSV または XML ファイルを作成します。
2. [Config] > [Tunnel Provisioning] の順に選択します。
3. [Assign Devices to Group] をクリックします。



4. [Browse] をクリックし、移動する FAR が含まれるファイルを検索します。
5. [Group] ドロップダウン メニューから、移動先のトンネル グループを選択します。
6. [Change Group] をクリックします。
7. [Close] をクリックします。

トンネル プロビジョニング テンプレートの設定

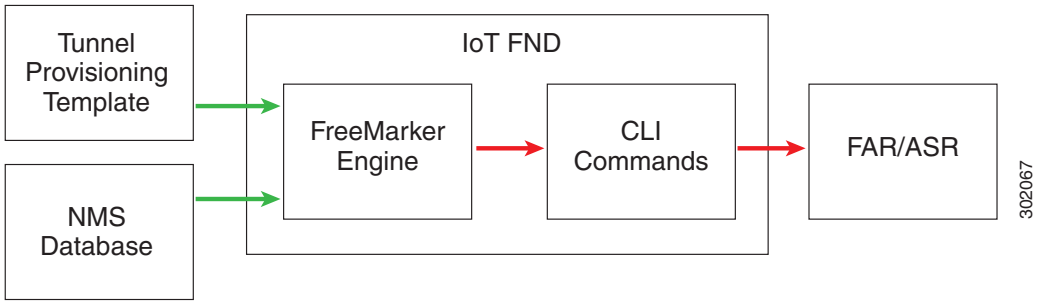
IoT FND には、デフォルトのトンネル プロビジョニング テンプレートが 3 つ含まれています。

- フィールド エリア ルータ トンネル追加：IoT FND はこのテンプレートを使用して FAR 上の IPsec トンネルの一端を作成するための CLI 設定コマンドを生成します。
- ヘッドエンド ルータ トンネル追加：IoT FND はこのテンプレートを使用して HER 上の IPsec トンネルの反対の端を作成するための CLI 設定コマンドを生成します。
- ヘッドエンド ルータ トンネル削除：IoT FND はこのテンプレートを使用して、トンネルの反対側にある FAR への既存のトンネルを削除するための CLI 設定コマンドを生成します。

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

IoT FND のトンネル プロビジョニング　テンプレートは FreeMarker のシンタックスで表されます。FreeMarker は、テンプレートを処理するための Java ベース オープン ソース エンジンで、IoT FND に組み込まれています。図 2 に示すとおり、FreeMarker は、入力として トンネル プロビジョニング テンプレートおよび IoT FND より提供されるデータを取得し、IoT FND が「configure terminal」コンテキストにおいて FAR と HER 上で実行する CLI コマンドを生成します。

図 2　IoT FND のテンプレートからの CLI コマンド生成



IoT FND では、トンネル プロビジョニング テンプレートはルータ CLI コマンド、FreeMarker の変数およびディレクティブで構成されています。FreeMarker のシンタックスを使用することにより、IoT FND は 1 つのテンプレートを定義して複数のルータをプロビジョニングすることができます。

ここでは、トンネル プロビジョニング テンプレートにおける FreeMarker の基本的なシンタックスについて説明します。FreeMarker について詳しくは、http://freemarker.sourceforge.net/ にアクセスしてください。

- テンプレートのシンタックス
- データ モデル

テンプレートのシンタックス

表 2 で、デフォルトのトンネル プロビジョニング テンプレートにおけるシンタックスについて説明します。

表 2　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

コンポーネント	説明
テキスト	標識のないテキストは FAR の CG-OS CLI 設定コマンド、HER の Cisco IOS CLI コマンドとして転送されます。
挿入	${variable} FreeMarker は、IoT FND によって提供される文字列変数の値とこの構成を置き換えます。この例では、IoT FNDは FAR の EID を提供します。 `description IPsec tunnel to ${far.eid}`
デフォルト値	${variable!" Default" } FreeMarker はこの構成を文字列変数の値で置き換えます。変数を設定しないと、FreeMarker は、この構成を **Default** で置き換えます。

条件	<#if condition> output1 <#else> output2 </#if>
	
	FreeMarker は出力で使用するテキストを決定するためにこの構成を使用します。次に例を示します。
	
	`<#if far.ipsecTunnelDestAddr1??>`
	`  <#assign destinationAddress=far.ipsecTunnelDestAddr1>`
	`<#else>`
	`  <#assign destinationAddress=`
	`her.interfaces("GigabitEthernet0/0/0")[0].v4.addresses[0].address>`
	`</#if>`

リスト上の反復	<#list list as variable> ${variable} </#list> FreeMarker はリスト上の反復にこの構造を使用します。
注	<#-- this is a comment --> FreeMarker ではコメントができますが、出力には保持されません。

表 2　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（続き）

コンポーネント	説明
ステートメントの指定	<#assign name=value> この構造は、テンプレート内のローカル変数を宣言し、それに値を割り当てます。その後、変数を参照するのにこの構成を使用します。 ${name} 次に例を示します。 <#assign **interfaceNumber**=0> ... interface Tunnel${**interfaceNumber**}

マクロ	これらの構成は関数呼出しに似ています。
	
	<#macro name(param1,param2, ... ,paramN)>
	
	... ${param1} ...
	
	</#macro>
	
	以下は、マクロ定義の例です。
	
	<#macro configureTunnel(interfaceNamePrefix,ospfCost)>
	  <#assign wanInterface=far.interfaces(interfaceNamePrefix)>
	  <#if (wanInterface[0].v4.addresses[0].address)??>
	  <#assign interfaceName=wanInterface[0].name>
	  interface Tunnel${her.unusedInterfaceNumber()}
	  description IPsec tunnel to ${far.eid}
	  ...
	  ip ospf cost ${ospfCost}
	  ...
	</#macro>

マクロ呼出し	トンネル プロビジョニング テンプレートでマクロを呼び出す方法： <@name param1, param2 ... paramN> FreeMarker は、すべての変数を解決した後、マクロ呼出しをマクロの出力と置き換えます。 次に例を示します。 <@configureTunnel far.tunnelSrcInterface1!"Wimax", 100/>

データ モデル

ここでは、トンネル プロビジョニング テンプレートにおけるデータ モデルについて説明します。**far** および **her** のプレフィックスはそれぞれ、FAR および HER のプロパティへのアクセスを提供します。これらのプロパティは IoT FND のデータベースに保存されています。表 3 では、トンネル プロビジョニング テンプレートのデータ モデルによって提供される情報の参照を示します。

表 3　データ モデル

プロパティ	説明
far.eid	FAR の EID を返します。次に例を示します。 ${**far.eid**}
far.hostname	FAR のホスト名を返します。

表 3　データ モデル(続き)

プロパティ	説明
far.tunnelSrcInterface1	トンネルを確立する FAR のインターフェイスの名前を返します。
far.ipsecTunnelDestAddr1	HER 上のトンネル宛先 IP アドレスの名前を返します。

far.ipv4Address(*clientId*, *linkAddress*, *userClass*)	IPv4 アドレスを返します。IPv4 アドレス メソッドはこれらのパラメータを入力として受け取ります。
	■ clientId:DHCP 要求の DCHP クライアント ID
	■ linkAddress:DHCP 要求のリンク アドレス
	■ userClass:DHCP ユーザー クラス オプション(デフォルトの「CG-NMS」)の値
	ループバック インターフェイスを確立し、それにアドレスを割り当てるには:
	`interface Loopback0`
	`ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32`
	`ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128`
	`exit`

far.ipv4Subnet()	DHCP IPv4 サブネット リースを返します。このコールは引数として clientId と linkAddress を取得します。 テンプレート API で提供される dhcpClientId() メソッドを使用して、FAR EID およびインターフェイス ID 番号から clientId を組み立てます。この方法では、入力として DHCPv6 アイデンティティ アソシエーション ID(IAID)および DHCP 固有 ID(DUID)を取得し、RFC 4361 に指定されるとおり DHCPv4 クライアント ID を生成します。この方法は、ネットワーク要素が DHCP サーバにより識別される方法に一貫性を与えます。 次に例を示します。 `<#assign lease=far.ipv4Subnet(dhcpClientId(far.enDuid,iaId), far.dhcpV4TunnelLink)>`
far.[any device property]	指定されたプロパティの値を返します。 たとえば、far.tunnelSrcInterface1 は FAR の tunnelSrcInterface1 プロパティの値を返します。

far.interfaces(interfaceNamePrefix)	そのプレフィックスをもつデバイスから検出されたインターフェイスのリストを返します(大文字と小文字の区別なし)。
	インデックス リストのメンバーには角カッコ、たとえば [0] [1] [2] を使用します。リストのメンバーを繰り返すには、<#list>構成を使用します。
	次に例を示します。
	`<#assign wanInterface = far.interfaces(interfaceNamePrefix)>`
	`  <#if (wanInterface[0].v4.addresses[0].address)??>`
	`...`

アドレス

表 4 で、トンネル プロビジョニング テンプレートで参照するアドレスを示します。

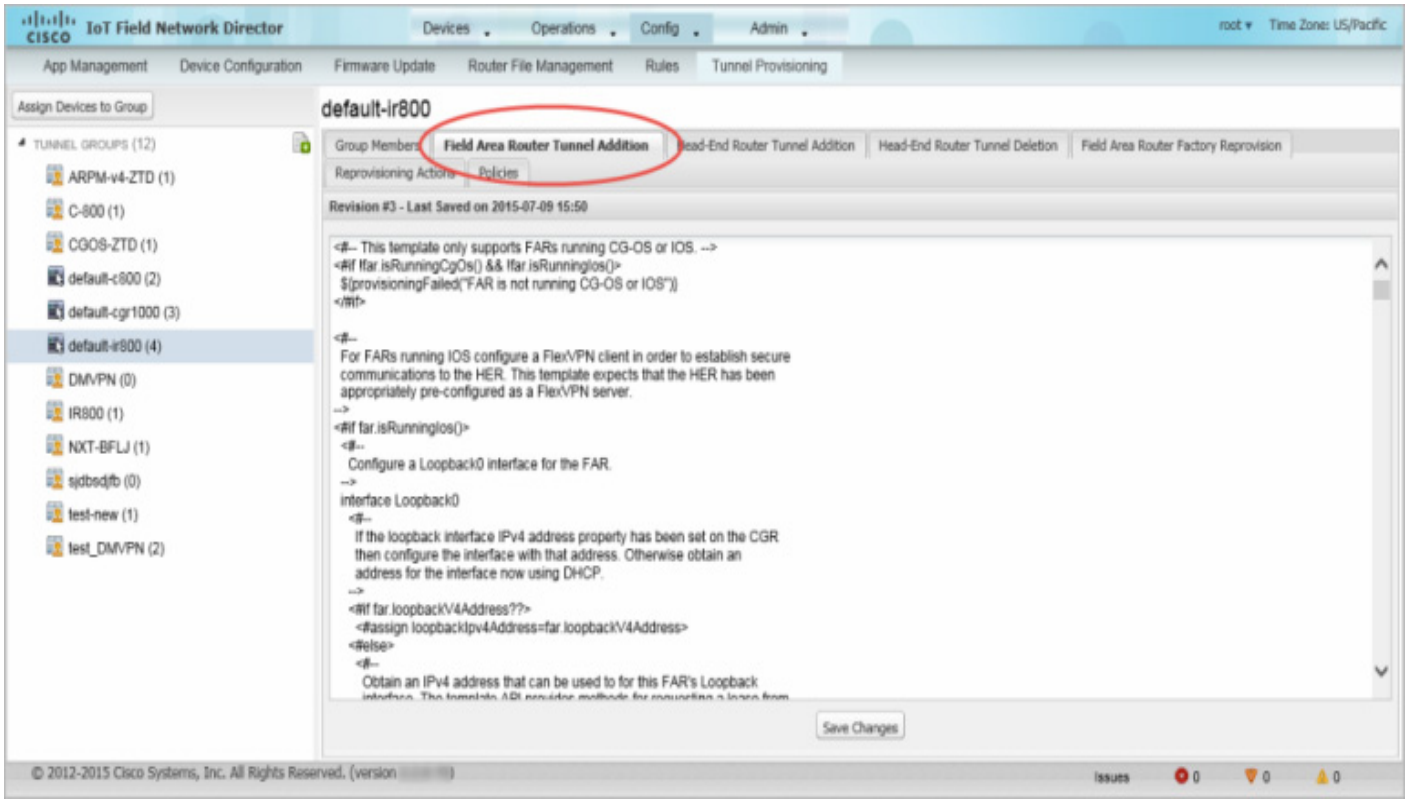
表 4　　参照アドレス

プロパティ	説明
address.address	インターフェイスのアドレスを返します。
address.prefixLength	アドレスのプレフィックス長が返されます。
address.prefix	アドレス プレフィックスを返します。
address.subnetMask	アドレスのサブネット マスクを返します。
address.wildcardMask	サブネットのワイルドカード マスクを返します。

フィールド エリア ルータ トンネル追加テンプレートの設定

FAR トンネル追加テンプレートを編集して、グループ内の FAR に IPsec トンネルの一方の端を作る方法:

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、編集するテンプレートのあるトンネル グループを選択します。
3. [Field Area Router Tunnel Addition] タブをクリックします。



4. デフォルトのテンプレートを変更します。

   ヒント:テンプレートを変更するには、テキスト エディタを使用し、テキストを IoT FND のテンプレート フィールドにコピーします。

5. [Save Changes] をクリックします。
6. [OK] をクリックして、変更内容を確定します。

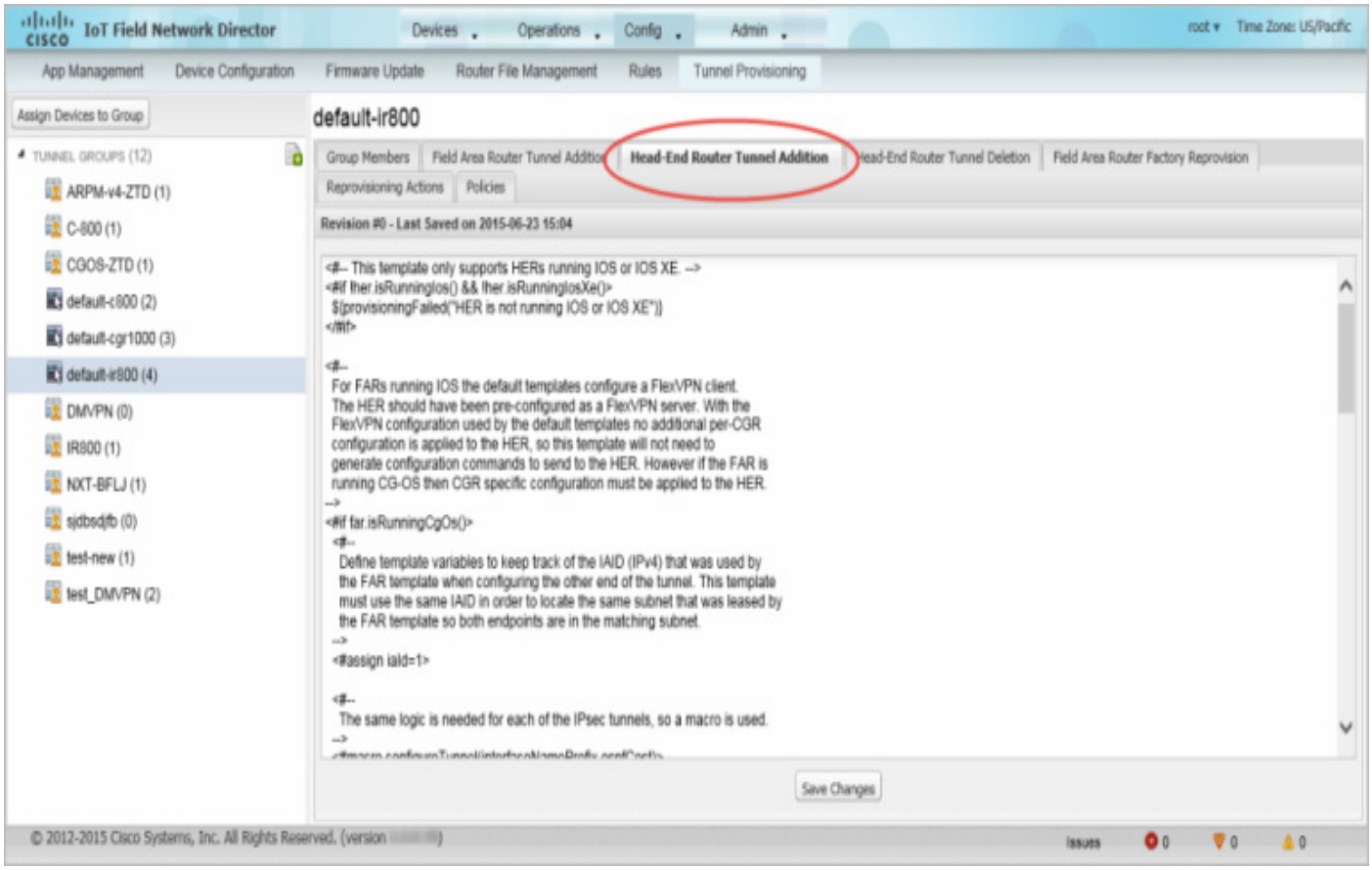
トンネル プロビジョニング テンプレートのシンタックスも参照してください。

ヘッドエンド ルータ トンネル追加テンプレートの設定

(注) 両エンドポイントが一致するサブネットにあることを確認するには、このテンプレートで FAR テンプレートと同じ IAID を使用する必要があります。

HER トンネル追加テンプレートを編集して、グループ内の HER に IPsec の反対側の端を作成する方法:

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、トンネル グループを選択します。
3. [Head-End Router Tunnel Addition] タブをクリックします。

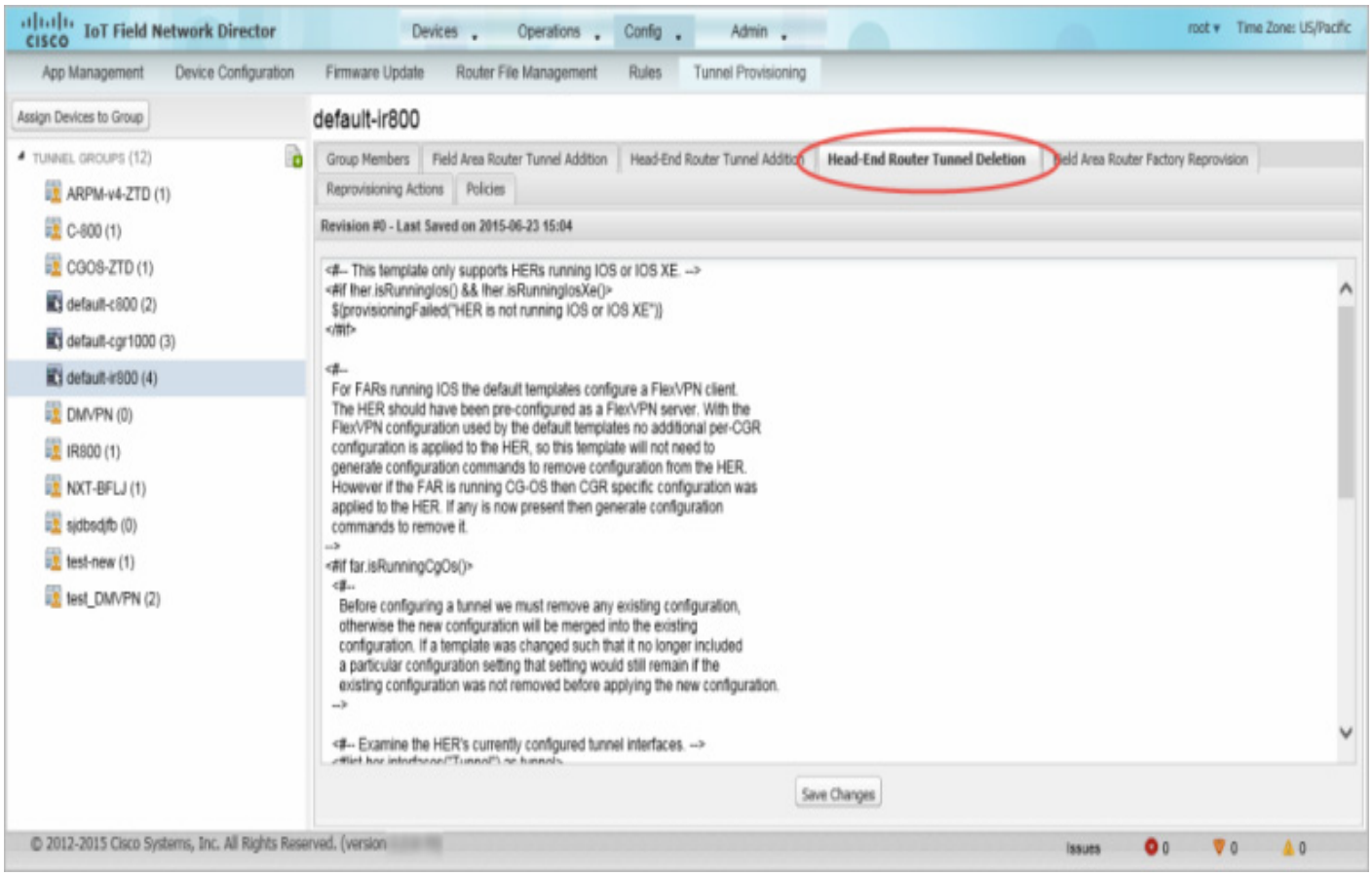


4. デフォルトの HER 追加テンプレートを変更します。
5. [Save Changes] をクリックします。
6. [OK] をクリックして、変更内容を確定します。

HER トンネル削除テンプレートの設定

HER トンネル削除テンプレートを編集して、トンネルの反対側にある FAR への既存のトンネルを削除する方法:

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを編集するトンネル グループを選択します。
3. [Head-End Router Tunnel Deletion] タブをクリックします。



4. デフォルトの HER 削除テンプレートを変更します。
5. [Save Changes] をクリックします。
6. [OK] をクリックして、変更内容を確定します。

トンネル ステータスのモニタリング

トンネルのステータスを表示するには、[Operations] > [Tunnel Status] の順に選択します。トンネル ステータスのページには、デバイスおよびプロビジョニングされたトンネルの一覧を表示し、トンネルおよびステータスに関する関連情報が表示されます。トンネルは HER と FAR の間にプロビジョニングされます。

ページ上部の [Show Filter] を選択すると、いくつかの検索フィールドが表示されます。表 5 に記載されているすべてのフィールド名でフィルタリングできます。1 つの検索フィールドに値を入力すると、使用できる他のフィールドが選択されます。検索フィールドを削除するには、[Hide Filter] を選択します。

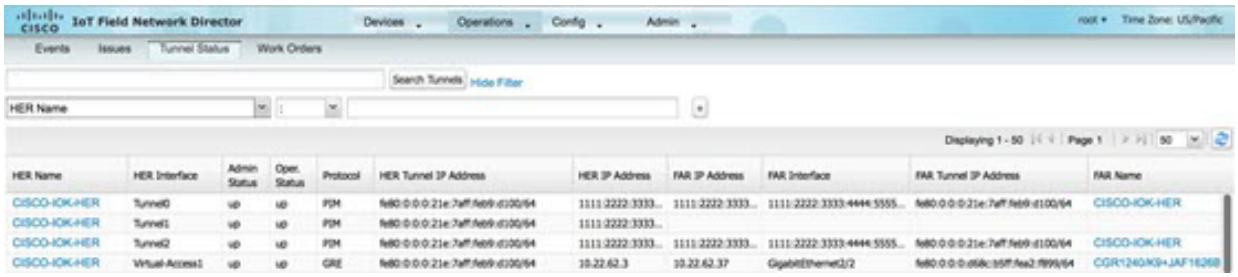


表 5 で、トンネル ステータス フィールドを示します。リスト内のトンネルのソート順序を名前で変更するには、[HER Name] カラムのヘッダーをクリックします。ヘッダーの横の小さな矢印がソート順を示します。

(注) 新しく作成されたトンネルのステータスが IoT FND に反映されるには時間がかかります

..

表 5　　トンネル ステータス フィールド

フィールド	説明
HER Name	トンネルの一方の端の HER の EID。HER の詳細を表示するには、その EID をクリックします。 (注) HER は 1 つが最大 500 の FAR を実行できるため、同じ HER EID をもつ複数のトンネルがリストにある可能性があります。 [Device Info] ページの [Network Interfaces] 領域には、HER に設定されたトンネルのリストが表示されます。[Config Properties] と [Running Config] タブには、この HER に設定されているトンネルに関する情報も含まれています。
HER Interface	HER トンネル インターフェイスの名前。これらの名前は、トンネルの作成時に自動的に生成されます (Tunnel1、Tunnel2、Tunnel3 など)。
Admin Status	トンネルの管理ステータス ([up] または [down])。これにより、管理者がトンネルを有効化または無効化したかが示されます。
Oper.Status (ステータス)	トンネルの動作ステータス ([up] または [down])。トンネルがダウンであれば、トラフィックは、トラブルシュートに問題を表示しているトンネルを通過しません。HER および FAR に ping を行ってオンラインであるか判断するか、SSH を介してルータにログインし、問題の原因を判断します。
Protocol	トンネルに使用されるプロトコル (IPSEC、PIM、GRE)。
HER Tunnel IP Address	HER 側のトンネルの IP アドレス。使用されるプロトコルにより、IP アドレスがドット付き 10 進法 (IPv4) または 16 進法 (IPv6) スラッシュ表記で表示されます。
HER IP Address	HER 側のトンネルの宛先 IP アドレス。
FAR IP Address	FAR 側のトンネルの宛先 IP アドレス。
FAR Interface	トンネルによって使用される FAR インターフェイスの名前。
FAR Tunnel IP Address	FAR 側のトンネルの IP アドレス。 (注) トンネルの両端の IP アドレスは同じサブネット上にあります。
FAR Name	FAR の EID。FAR の詳細を表示するには、その EID をクリックします。 [Device Info] ページの [Network Interfaces] 領域には、FAR に設定されたトンネルのリストが表示されます。[Config Properties] と [Running Config] タブには、この FAR に設定されているトンネルに関する情報も含まれています。

CGR のプロビジョニング

IoT FND では、CGR 再プロビジョニングは CGR の設定ファイルを変更するプロセスです。

- CGR 再プロビジョニングの基本
- トンネル再プロビジョニング
- 出荷時再プロビジョニング

(注) C800 は再プロビジョニングをサポートしていません。

CGR 再プロビジョニングの基本

- CGR 再プロビジョニングのアクション
- CGR 再プロビジョニングのシーケンス

CGR 再プロビジョニングのアクション

IoT FND では、[Tunnel Provisioning] ページの [Reprovisioning Actions] ペインで以下の 2 つの CGR 再プロビジョニング アクションを実行できます ([Config] > [Tunnel Provisioning])。

また、このページでメッシュ ファームウェアを有効化することができます。

再プロビジョニング アクション	説明
出荷時再プロビジョニング	工場出荷時の設定時に CGR にロードされた express-setup-config ファイルを変更します。 このファイルには、最小限の情報セットが含まれており、出荷時に CGR にロードされます。このファイルは、CGR が展開されて電源がオンになった後、TPS プロキシ経由で IoT FND にコンタクト (Call Home) するための情報を提供します。
トンネル再プロビジョニング	CGR の golden-config ファイルを変更します。このファイルには CGR に定義されたトンネル 構成があります。

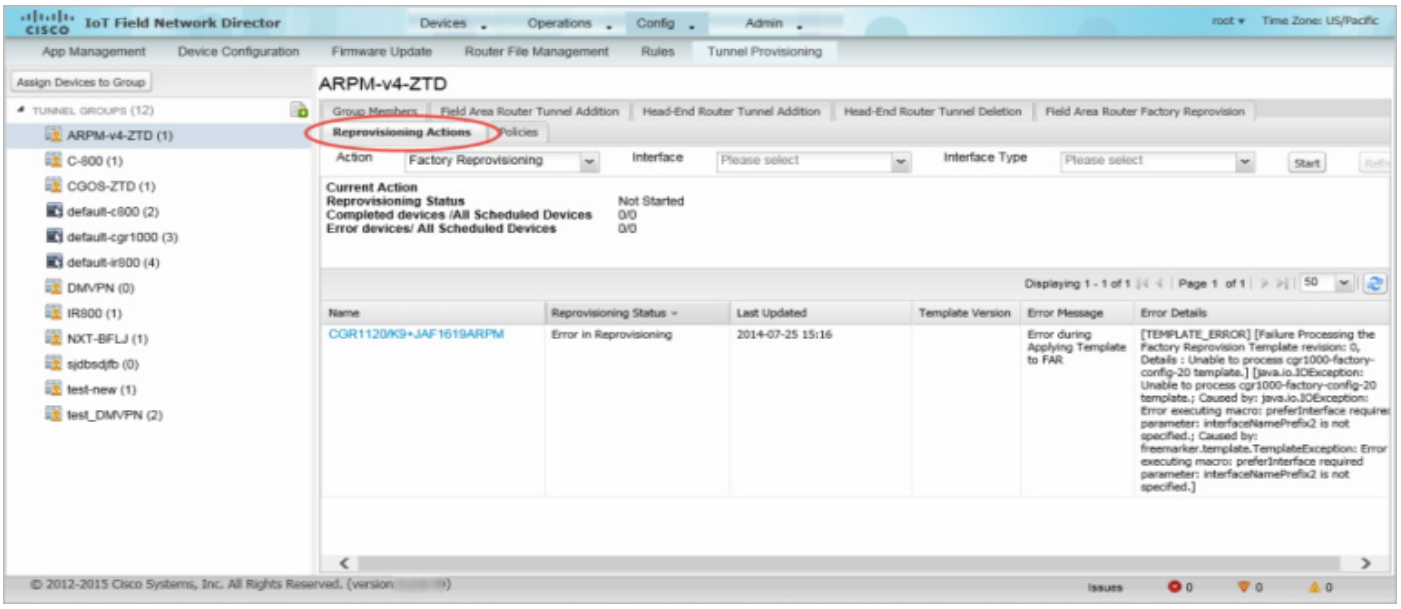


表 6 で、[Reprovisioning Actions] ペインのフィールドについて説明します。

表 6　[Reprovisioning Actions] ペインのフィールド

フィールド	説明
Current Action	現在実行中の再プロビジョニング アクション。
Reprovisioning Status	再プロビジョニング アクションのステータス。
Completed devices /All Scheduled Devices	プロセスがスケジュール設定されたすべての CGR の数に対し、処理された CGR の数。
Error devices/ All Scheduled Devices	プロセスがスケジュール設定されたすべての CGR の数に対し、エラーを報告した CGR の数。
名前	CGR の EID。
Reprovisioning Status	この CGR の再プロビジョニング アクションのステータス。
Last Updated	この CGR の再プロビジョニング アクションのステータスが最後に更新された時間。
Template Version	適用されるフィールド エリア ルータの出荷時再プロビジョニング テンプレートのバージョン。
エラー メッセージ	CGR によって報告されたエラー メッセージ(ある場合)。
Error Details	エラーの詳細。

CGR 再プロビジョニングのシーケンス

トンネル プロビジョニング グループに対してトンネル再プロビジョニングまたは出荷時再プロビジョニングを開始すると、再プロビジョニング アルゴリズムが一度に 12 の CGR を連続して処理し、再プロビジョニングします。

IoT FND が正常にルータを再プロビジョニングした後、またはエラーが報告されると、IoT FND はグループ内の次のルータの再プロビジョニング プロセスを開始します。すべての CGR が再プロビジョニングされるまで、IoT FND はこのプロセスを繰り返します。

グループ内の各 CGR を再プロビジョニングする場合、4 時間でタイムアウトします。CGR が正常な再プロビジョニングを報告しなかったり、タイムアウト時間内にエラーがあった場合、IoT FND は CGR の再プロビジョニングのステータスを [Error] に変更し、タイムアウト エラーを表示します。その他の詳細情報はすべて、[Error Details] フィールドに表示されます。

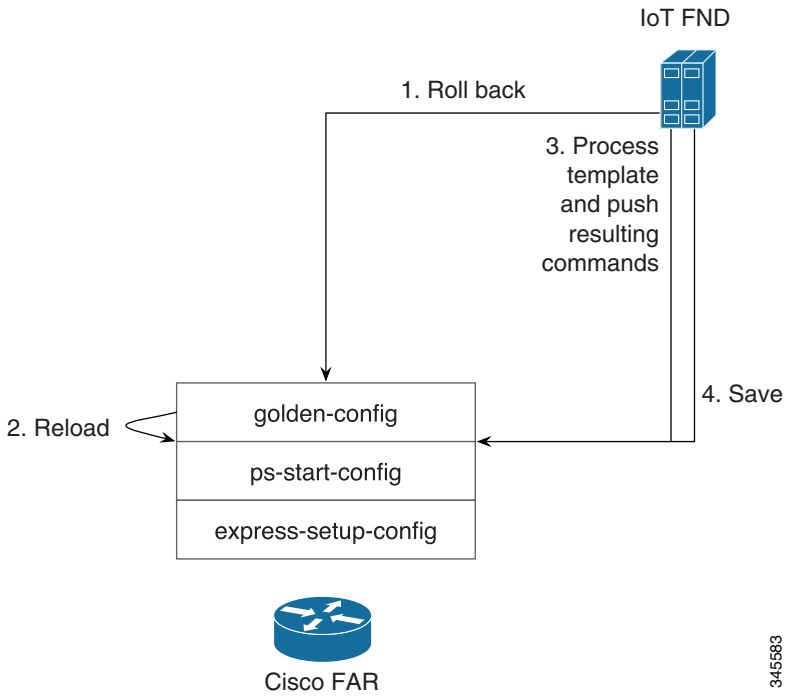
トンネル再プロビジョニング

フィールド エリア ルータ トンネル追加テンプレートを変更し、すでに IoT FND に接続したすべての CGR を変更されたテンプレートに基づく新しいトンネルで再プロビジョニングする場合、IoT FND のトンネル再プロビジョニング機能を使用します。

トンネル再プロビジョニングは、CGR をトンネルが設定されていない状態にし、その後、新しいトンネル プロビジョニング要求を開始します。トンネルを再プロビジョニングするため、IoT FND はトンネル プロビジョニング グループ内の FAR を連続して処理します(一度に 12)。各 CGR に対し、IoT FND は CGR の構成を ps-start-config テンプレート ファイルに定義された状態にロールバックします。

ps-start-config へのロールバックの後、CGR は IoT FND にコンタクトしてトンネル プロビジョニングを要求します。IoT FND はフィールド エリア ルータ トンネル追加テンプレートを処理し、その結果として得られた新しいトンネル作成の設定コマンドを CGR に送信します。図 3 に示すとおり、トンネル プロビジョニング プロセスには、新しい設定情報が含まれるよう golden-config ファイルを更新することが含まれます。

図 3　トンネル再プロビジョニング プロセス



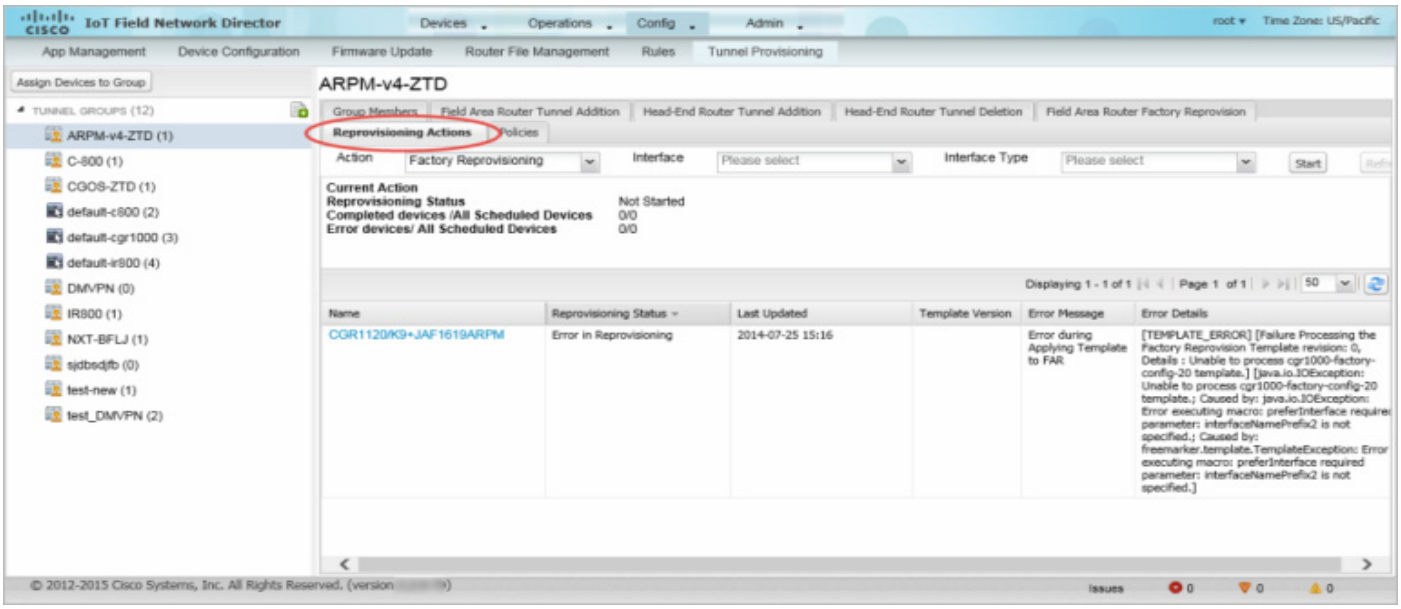
(注) CG-OS CGR では、ロールバックにより CGR がリロードされます。また、IoT FND が CGR をロールバックすると、IoT FND は対応するトンネル情報を CGR が接続された HER から削除します。

Cisco IOS ベースの CGR に構成の置換を実行します。

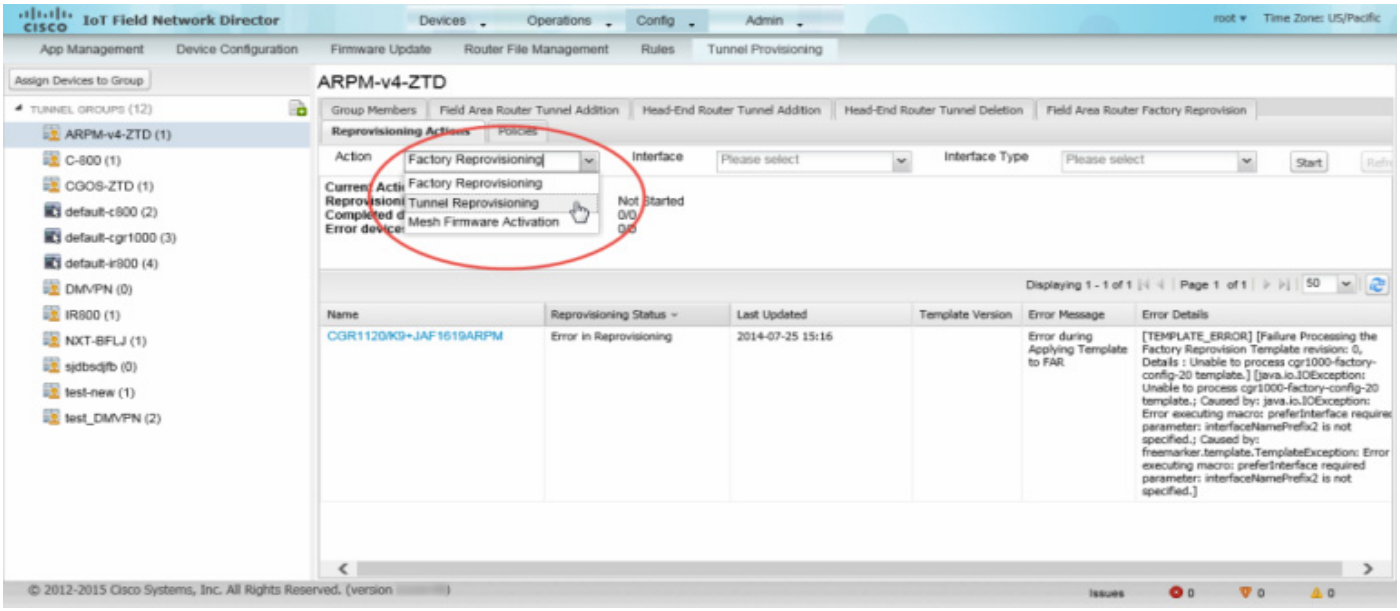
(注) フィールド エリア ルータ出荷時再プロビジョニング テンプレートは、トンネル再プロビジョニングの実行時には使用されません。

トンネル再プロビジョニングを設定してトリガーする方法:

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを再プロビジョニングするトンネル グループを選択します。
3. [Reprovisioning Actions] タブをクリックします。



4. [Action] ドロップダウン メニューから、[Tunnel Reprovisioning] を選択します。



5. [Start] をクリックします。

IoT FND は [Reprovisioning Status] フィールドを [Initialized] に変更し、次に [Running] に変更します。

(注) トンネル再プロビジョニングの実行中に [Stop] をクリックすると、IoT FND は選択されなかったキューの FAR についてのみ、再プロビジョニング プロセスを停止します。ただし、再プロビジョニングを選択したキューの CGR に関しては、プロセスは完了され（正常またはエラー）、停止することはできません。

再プロビジョニング プロセスは、IoT FND がトンネル プロビジョニング グループ内の各 CGR を再プロビジョニングする試みを終了した後、完了します。CGR が 1 つでも再プロビジョニングできなければ、IoT FND は CGR が報告したエラー メッセージを表示します。

出荷時再プロビジョニング

IoT FND の出荷時再プロビジョニング機能を使って、CGR の工場出荷時の設定（express-setup-config）を変更します。

出荷時再プロビジョニングでは次の手順を行います。

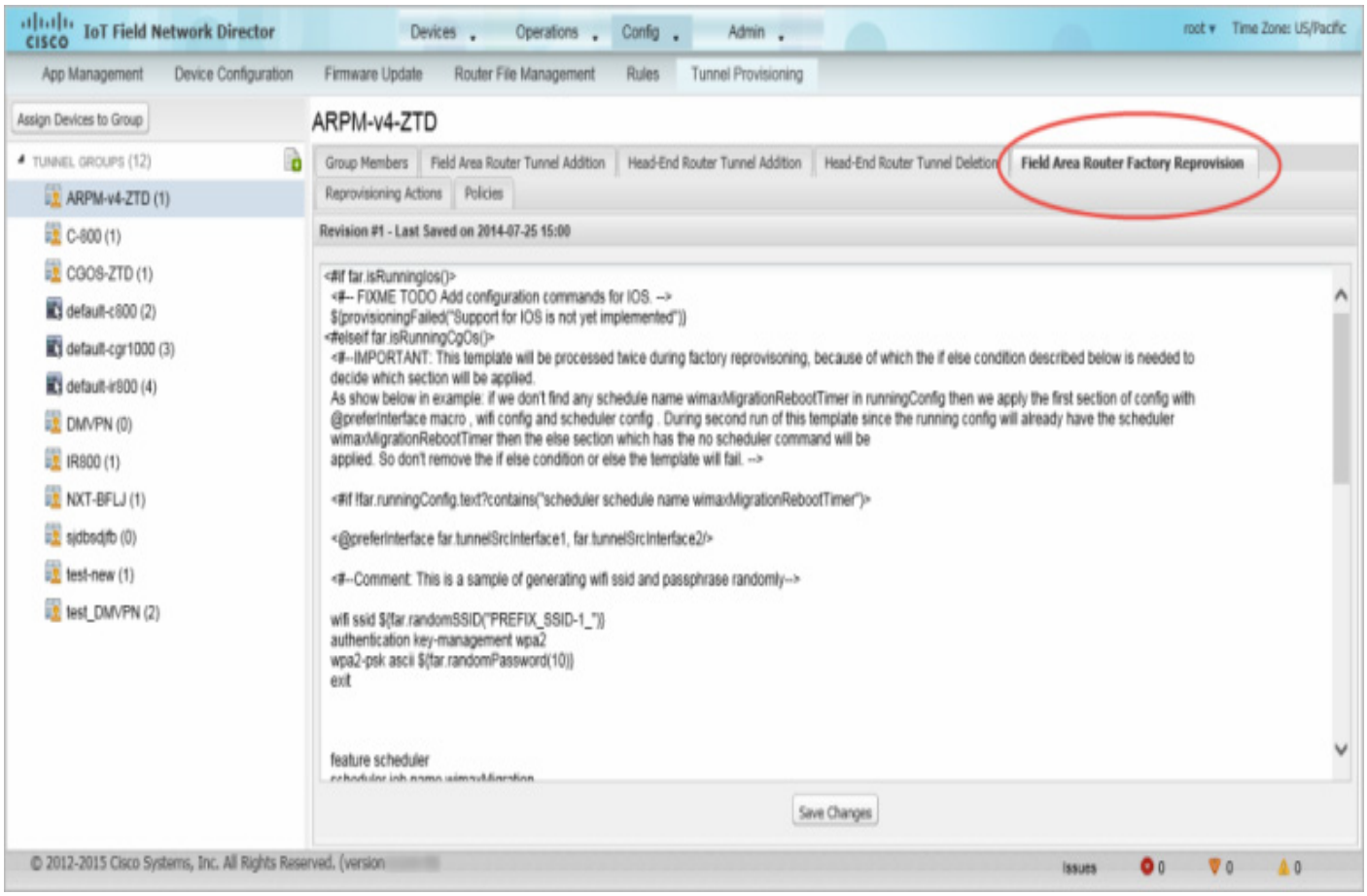
1. CGR にロールバック コマンドを送信します。
2. CGR をリロードします。
3. フィールド エリア ルータ出荷時再プロビジョニング テンプレートを処理し、結果として得られたコマンドを CGR にプッシュします。
4. express-setup-config ファイルの構成を保存します。

これらの手順が正常に完了した後、IoT FND はフィールド エリア ルータ トンネル追加、ヘッドエンド ルータ トンネル追加、およびヘッドエンド ルータ トンネル削除の各テンプレートを処理し、結果として得られたコマンドを CGR にプッシュします（トンネル プロビジョニング設定プロセス参照）。

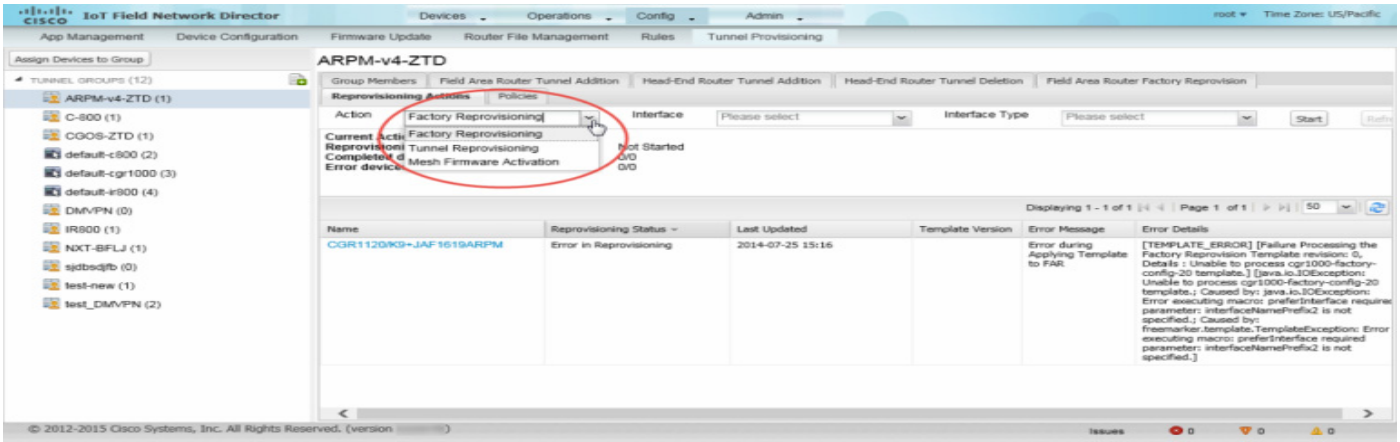
出荷時再プロビジョニングを設定してトリガーする方法：

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを編集するトンネル グループを選択します。
3. [Field Area Router Factory Reprovision] タブをクリックし、適用する設定コマンドを含むテンプレートを入力します。

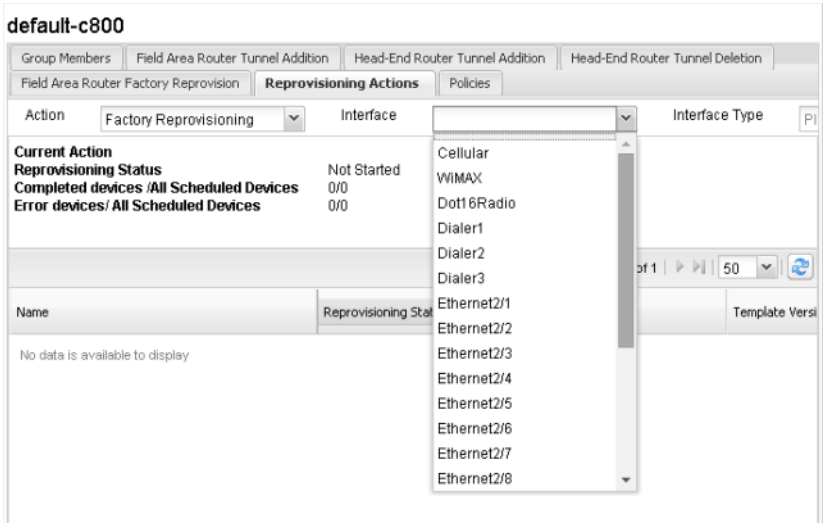
   (注) このフィールド エリア ルータ出荷時再プロビジョニング テンプレートは出荷時再プロビジョニングの間に 2 回処理されます。設定をプッシュするときに 1 回、設定を express-setup-config に保存する前にもう 1 回です。この理由により、個人的にテンプレートを作るときは、デフォルトのテンプレートで定義された特定の if/else 条件モデルを使用してください。



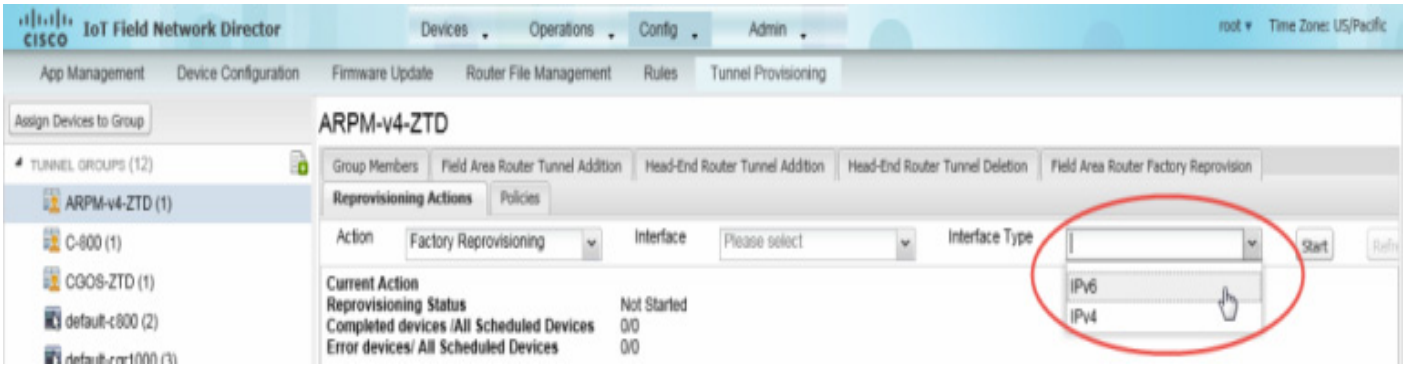
4. [Save Changes] をクリックします。
5. 必要に応じて、フィールド エリア ルータ トンネル追加、ヘッドエンド ルータ トンネル追加、およびヘッドエンド ルータ トンネル削除の各テンプレートに必要な変更を加えます。
6. [Reprovisioning Actions] タブをクリックします。
7. [Action] ドロップダウン メニューから、[Factory Reprovisioning] を選択します。



8. [Interface] ドロップダウン メニューから、再プロビジョニングのため FAR との接続に使用するIoT FND の CGR インターフェイスを選択します。



9. [Interface Type] ドロップダウン メニューから [IPv4] または [IPv6] を選択します。



10. [Start] ボタンをクリックします。

    IoT FND は [Reprovisioning Status] フィールドを [Initialized] に変更し、次に [Running] に変更します。

    (注) 出荷時再プロビジョニング実行中に [Stop] をクリックすると、IoT FND は選択されなかったキューの FAR についてのみ、再プロビジョニング プロセスを停止します。ただし、再プロビジョニングを選択したキューの CGR に関しては、プロセスは完了され、停止することはできません。

再プロビジョニング プロセスは、IoT FND がトンネル プロビジョニング グループ内の各 CGR を再プロビジョニングする試みを終了した後、完了します。CGR が 1 つでも再プロビジョニングできなければ、IoT FND は CGR が報告したエラー メッセージを表示します。

フィールド エリア ルータ出荷時再プロビジョニング　テンプレートの例

このテンプレートの例は、工場出荷時構成の WiFi SSID およびパスフレーズを変更します。

```
<#--IMPORTANT: This template is processed twice during factory reprovisioning.The if/else condition
described below is needed to determine which part of the template is applied.
In this example, if no schedule name wimaxMigrationRebootTimer is found in runningConfig, then the if
part of the if/else section is applied.During the second pass, this template runs the commands in the
else section and the no scheduler command is applied.If modifying this template, do not remove the
if/else condition or else the template fails.-->

<#if !far.runningConfig.text?contains("scheduler schedule name wimaxMigrationRebootTimer")>

<#--Comment: This is a sample of generating wifi ssid and passphrase randomly-->

wifi ssid ${far.randomSSID("PREFIX_")}
authentication key-management wpa2
wpa2-psk ascii ${far.randomPassword(10)}
exit

feature scheduler
scheduler job name wimaxMigration
reload
exit

scheduler schedule name wimaxMigrationRebootTimer
time start +02:00
job name wimaxMigration
exit

<#else>

no scheduler job name wimaxMigration
no scheduler schedule name wimaxMigrationRebootTimer

</#if>
```

モニタリング システム アクティビティ

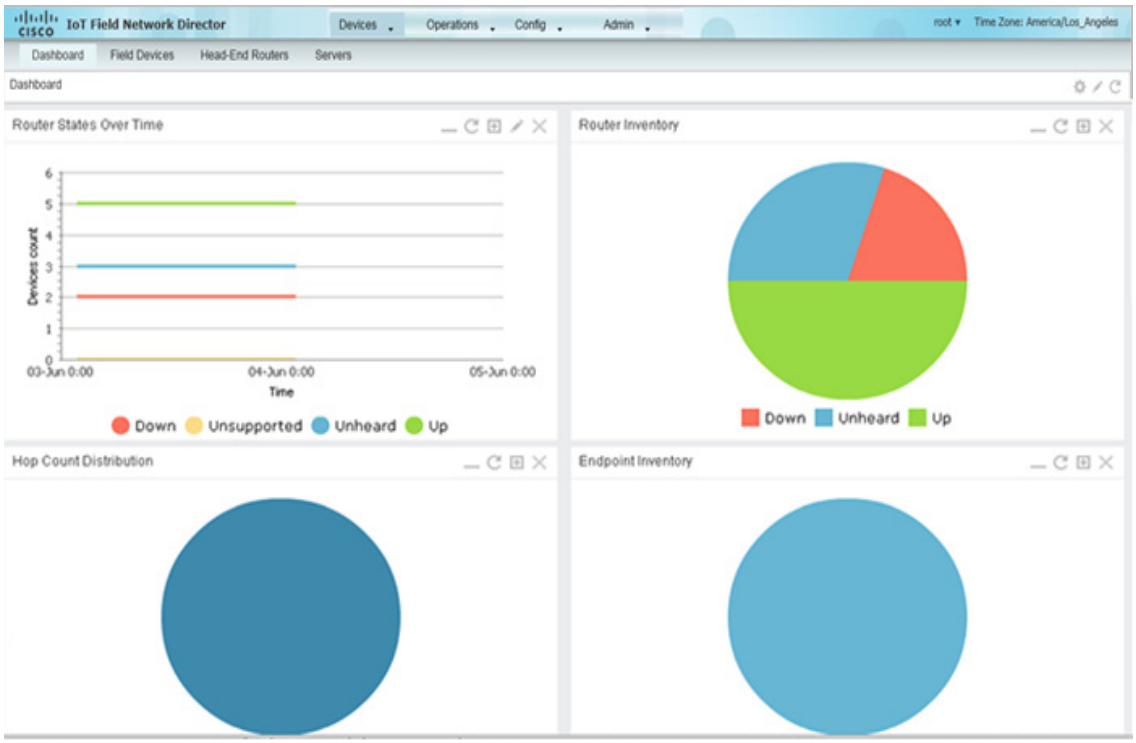
この項では、IoT FND システム アクティビティをモニタする方法について説明します。次の項目を取り上げます。

- ダッシュボードの使用
- イベントのモニタリング
- モニタリングの問題
- デバイス グラフの表示

ダッシュボードの使用

IoT FND ダッシュボード(図 1)には、重要なネットワーク メトリックの概要をビジュアルに示すダッシュレットが表示されます。

図 1　　IoT FND ダッシュボード



このセクションでは、次のダッシュボードの機能について説明します。

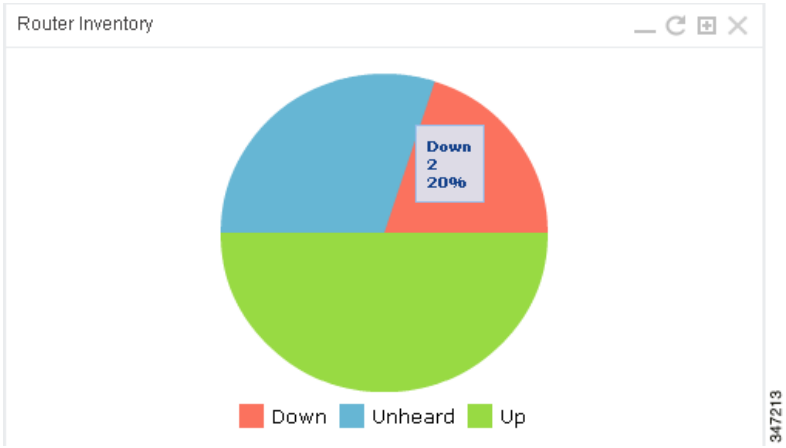
- ダッシュレットのタイプ
- ダッシュレットの位置変更

- ダッシュレットの更新間隔の設定
- ダッシュレットの追加
- ダッシュレットの削除
- ダッシュレット データのエクスポート

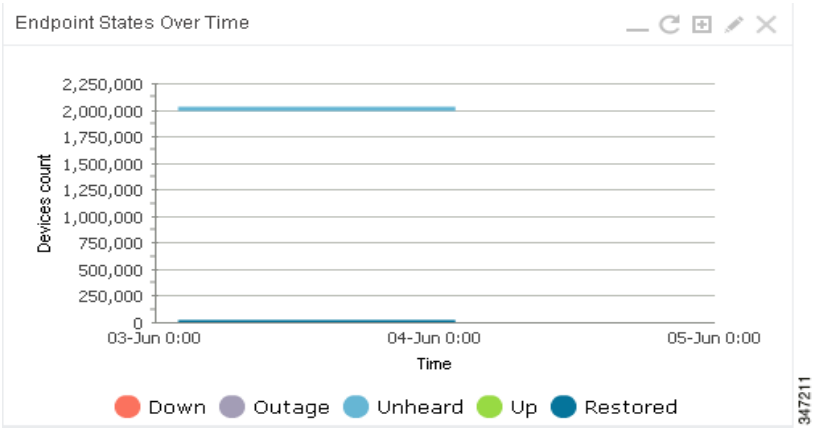
ダッシュレットのタイプ

ダッシュボードには、次の 2 つのタイプのダッシュレットが表示されます。

- 円グラフ ダッシュレットには、円グラフでデバイスのプロパティの割合が表示されます。



- 線グラフ ダッシュレットには、時間の経過に応じたデバイス数を表示するグラフが表示されます。



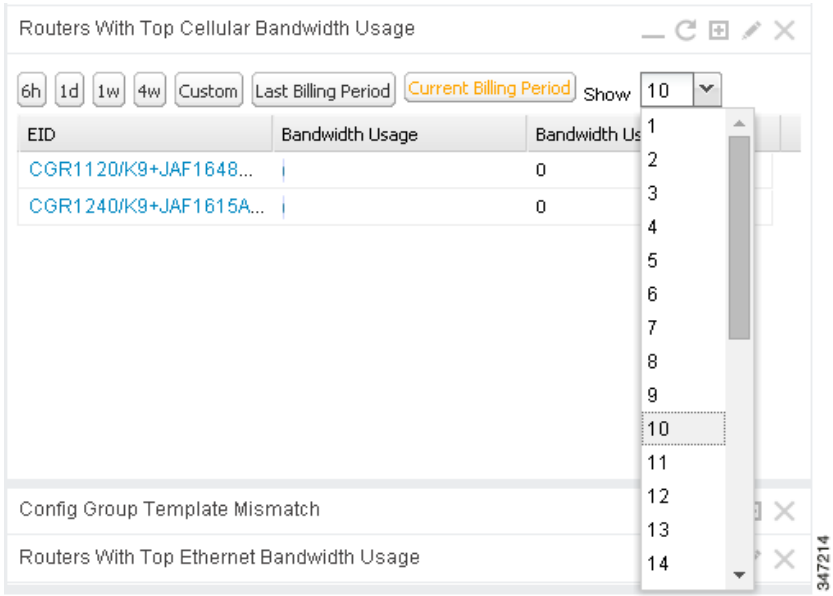
ヒント:1 日より長い間隔に設定されているグラフでは、[Device Info] ページ上の対応するフィールドに示されているとおりの最終データポイントでデータが正確に表示されない場合があります。これは、[Device Info] ページのフィールドを更新するためのポーリングよりも少ない頻度でデータ集約が実行されているためです。データがさらに高い頻度で更新されるように、それらのグラフを 6 時間～ 1 日の間隔に設定してください。1 日より長い間隔でデータのトレンドを表示します。

ダッシュボード ダッシュレット

ここから、IoT FND ダッシュボード ダッシュレットについて説明します。

ダッシュレット	説明
Router Inventory	この FAR ステータス カウントの円グラフには、FAR のステータス分布と絶対カウントが表示されます。
Router States Over Time	この線グラフは、設定されている時間間隔内の FAR の数とその状態を示します。
エンドポイント インベントリ	このエンドポイントの状態には、エンドポイントの割合（および数）が表示されます。たとえば、Unheard と、Up、Down、および Outage などの他の状態と比較したデバイスの数などです。
Endpoint States Over Time	この線グラフは、設定されている時間間隔内のエンドポイントの数とその状態を示します。
Endpoint Config Group Template Mismatch Over Time	この線グラフは、すべての設定グループと、設定されている時間間隔に同期していない特定の設定グループの、エンドポイント数を示します。
Endpoint Firmware Group Membership Mismatch Over Time	この線グラフは、すべてのファームウェア グループと、設定されている時間間隔に同期していない特定のファームウェア グループの、エンドポイント数を示します。
Config Group Template Mismatch	この円グラフは、設定グループ テンプレートが一致または不一致のデバイス数を示します（ME 設定グループにのみ適用可能）。
Firmware Group Membership Mismatch	この円グラフは、ファームウェア グループが一致しないデバイスの数を示します（エンドポイント ファームウェア グループにのみ適用可能）。
Hop Count Distribution	この円グラフは、メッシュ デバイスのホップ数分布を示します。
Service Providers with Maximum Down Routers for Cellular 1	このダッシュレットは、シングル モデム ルータのデバイス タイプ CGR1000、C800 および IR800 におけるダウンしているルータの集約された最大数を表示します。
Service Providers with Maximum Down Routers for Cellular 2	このダッシュレットは、デュアル モデム ルータのデバイス タイプ CGR1000、C800 および IR800 におけるダウンしているルータの集約された最大数を表示します。
Service Providers with Maximum Routers	このダッシュレットは、サービス プロバイダ名、その関連セル ID（入手可能な場合）、その関連ルータ合計数、およびダウンしているルータの数を示します。さらにこのダッシュレットは、時間の経過に応じた帯域幅の使用と、ダウンしているルータを示すスパーク線を表示します。 ヒント：任意のカラム見出しの三角形をクリックし、コンテキスト メニューで [Columns] を選択し、[Down Routers Over Time] チェックボックスをオンにすると、このカラムは非表示になります。

ダッシュレット	説明
Routers With Top Cellular Bandwidth Usage	この帯域幅グラフは、セルラー帯域幅を最も多く使用している上位 *n* 個のルータを表示します。ここで *n* は、表示される上位ルータの数です。また、各セルラー インターフェイスを示します。[Filter] ボタンをクリックして、[Show] ドロップダウン リストから、表示するルータの数を選択します。



- [Last Billing Period] ボタンをクリックすると、最終の請求期間に帯域幅を最も多く使用した上位 *n* 個のルータの帯域幅使用情報が表示されます。
- [Current Billing Period] ボタンをクリックすると、現在の請求期間の帯域幅使用情報が表示されます。

  開始日は、[Billing Period Settings] タブ（[Admin] > [System Management] > [Server Settings]）で定義されます。

Routers With Top Ethernet Bandwidth Usage	このダッシュレットは、[Routers With Top Cellular Bandwidth Usage] ダッシュレットと似ていますが、イーサネット帯域幅を最も多く使用している上位 *n* 個のルータを表示する点が異なります。
Routers With Least Cellular RSSI	このダッシュレットは、最後のポーリングで最低の RSSI 値を示したルータのグラフを表示します。これは信号強度の品質と、各セルラー インターフェイスを示します。このグラフは、FAR のセルラー チャネル状態を測定するために使用します。

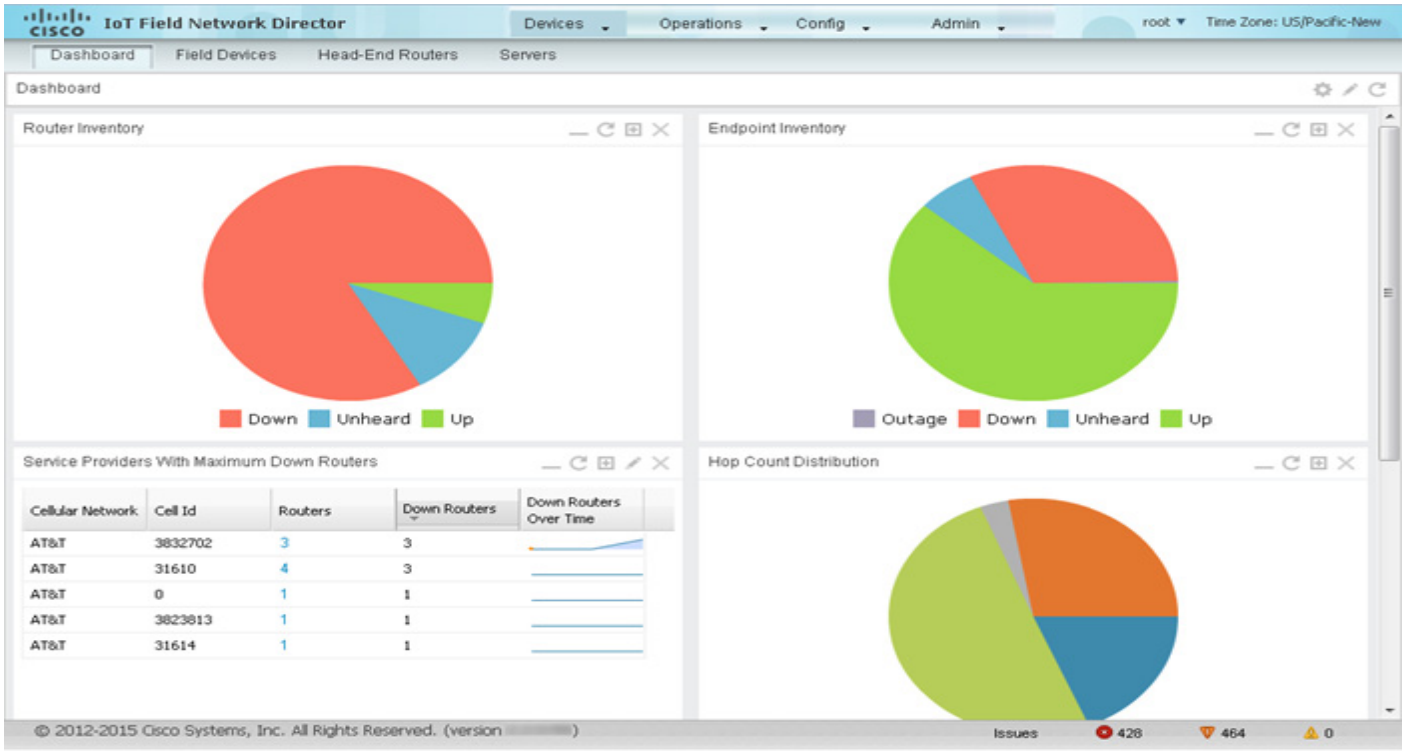
ダッシュレットの位置変更

ダッシュボードは、ユーザの好みに合わせた配置でグラフを表示するためにカスタマイズできます。ダッシュボードを設定するには、次の手順を実行します。

- グラフのタイトル バーをクリックして、好みの位置にドラッグします。
- ページからグラフを削除するには、クローズ ボックスをクリックします。
- 間隔を指定するボタンをクリックして、次のことを実行します。
  - 線グラフを表示する間隔を定義します。
  - 線グラフを表示するカスタム間隔を定義します。
  - 線グラフに表示するデバイスの数を選択します。
  - 線グラフに表示するデータを絞り込むシリーズを選択します。
  - 線グラフの表示をグループでフィルタリングします。
- タイトル バーの [Settings] ボタンをクリックして、すべてのグラフの更新間隔を設定し、ダッシュレットをダッシュボードに追加します。

ダッシュボードの下部のダッシュレットをさらに見やすく表示するには、ダッシュレットの表示/非表示ボタン( )をクリックして、ダッシュレットをそのタイトル バーにまで折りたたみます。図 2 では、[Config Group Template Mismatch] ダッシュレットがダッシュボード内で展開されており、他のいくつかのダッシュレットはその上に折りたたまれています。ダッシュボードを更新するには、[Refresh] ボタン( )をクリックします。ダッシュレットを更新するには、[Refresh] ボタンをクリックします。

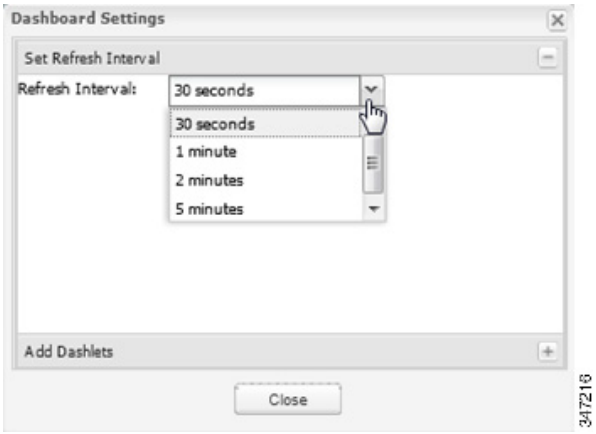
図 2　　折りたたまれたダッシュレットがあるダッシュボード



ダッシュレットの更新間隔の設定

ダッシュレットの更新間隔を設定するには、次の手順を実行します。

1. [Devices] > [Dashboard] を選択します。
2. [Settings] ボタン( )をクリックします。
3. [Set Refresh Interval] をクリックします。



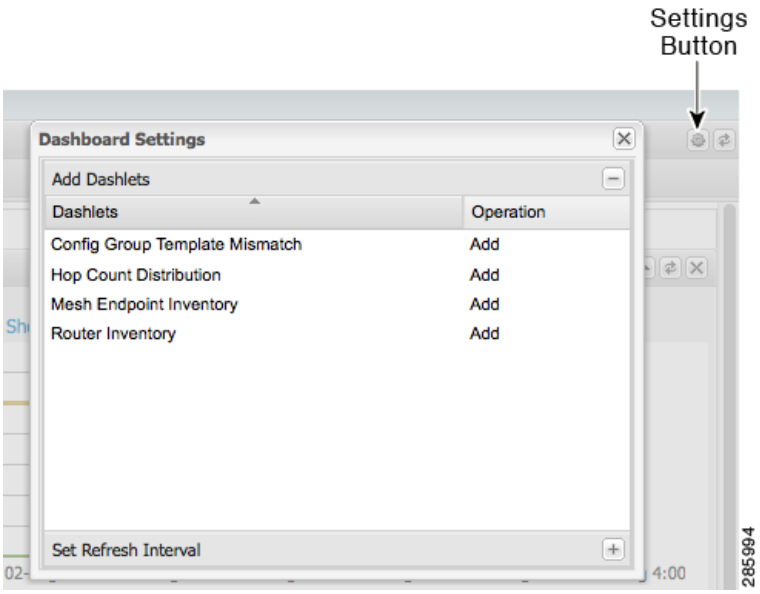
(注)線グラフのダッシュレットでは、フィルタ バーを開いて間隔を指定するボタンをクリックすると、その期間のメトリックが表示されます。

4. ドロップダウン メニューから、更新間隔を選択します。
5. 終了したら、[Dashboard Settings] ダイアログボックスを閉じます。

ダッシュレットの追加

ダッシュボードにダッシュレットを追加するには、次の手順を実行します。

1. [Devices] > [Dashboard] を選択します。
2. [Settings] ボタン( )をクリックします。



3. [Add Dashlet] をクリックします。

   (注)すべてのダッシュレットがダッシュボード上に表示されている場合は、このダイアログ ボックスに表示されるダッシュレットはありません。

4. ダッシュレットをクリックして、ダッシュボードに追加します。

5. 終了したら、[Dashboard Settings] ダイアログボックスを閉じます。

ダッシュレットの削除

ダッシュボードからダッシュレットを削除するには、次の手順を実行します。

1. [Devices] > [Dashboard] を選択します。

2. ダッシュレットの [Close] ボタンをクリックします。

詳細を表示するための円グラフの使用

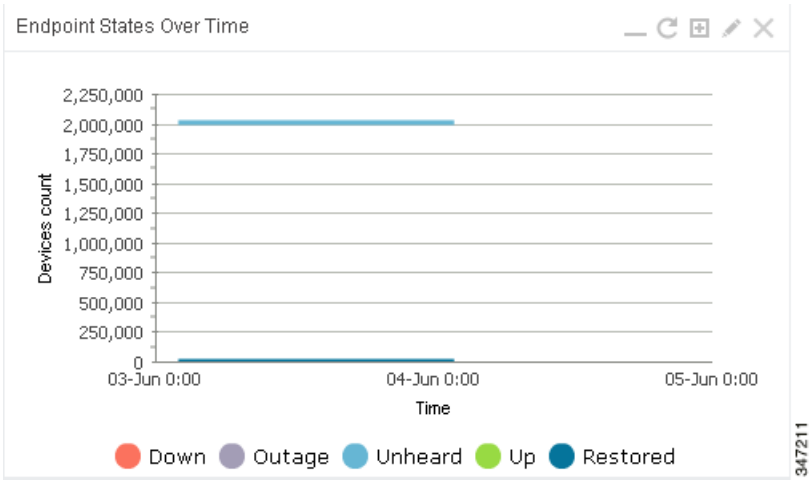
コールアウトとそのセグメントの情報を表示するには、円グラフの任意のセグメントにマウス オーバーします。[Router Inventory] と [Mesh Endpoint Inventory] 円グラフの任意のセグメントをクリックして、リスト ビューにデバイスを表示します。

ダッシュレットの時間プロパティの設定

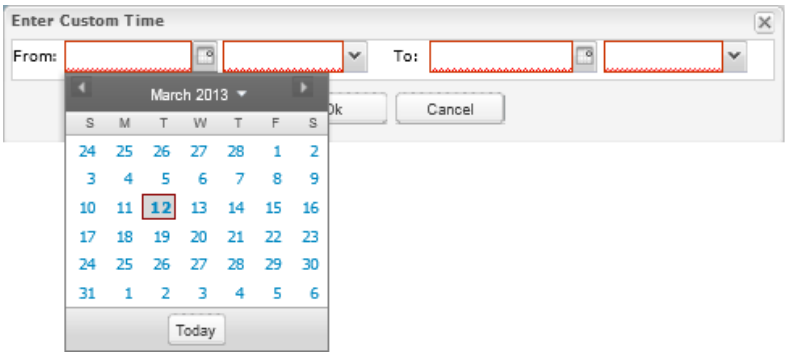
線グラフ ダッシュレットのデータ収集の時間間隔を指定するには、タイトル バーの間隔アイコン( )をクリックして、[6h]、[1d]、[1w]、[4w]、または [Custom] ボタンをクリックします。 [6h] ボタンは、データ収集時間間隔を直近の 6 時間に設定します。[1d] ボタンは、時間間隔を直近の 24 時間に設定します。

線グラフ ダッシュレットのカスタム時間間隔を指定するには、次の手順を実行します。

1. [Custom] をクリックします。



2. [From] フィールドに、開始日時を指定します。



3. [To] フィールドに、終了日時を指定します。
4. [OK] をクリックします。

ダッシュレットの折りたたみ

ダッシュレットをそのタイトル バーに折りたたむには、右上にある表示/非表示アイコン( )をクリックします。

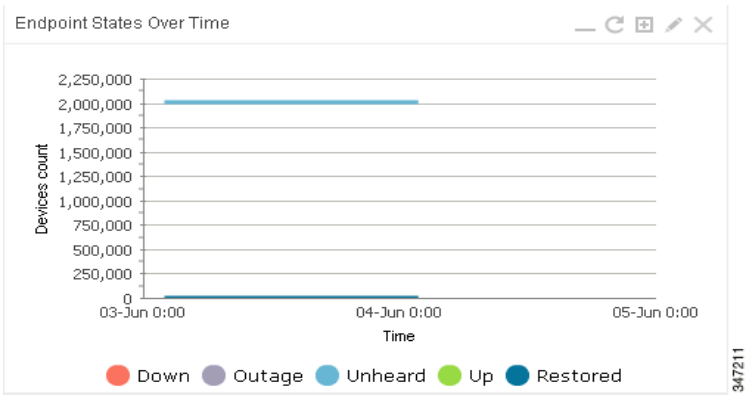
シリーズ セレクタの使用

線グラフをデバイスのステータス別に表示されるように調整するには、シリーズ セレクタを使用します。デバイスのオプションは、次のとおりです。

- ルータ：Down、Outage、Unsupported、Unheard、および Up
- メッシュ エンドポイント設定グループ：Config Out of Sync、Config In Sync
- メッシュ エンドポイント ファームウェア グループ：Membership Out of Sync、Membership In Sync
- メッシュ エンドポイント ステータス：Down、Outage、Unheard、Up

シリーズ セレクタを使用するには、次の手順を実行します。

1. [Series Selector] をクリックします。



2. [Series Selector] ダイアログ ボックスで、グラフに表示するデータ シリーズのチェックボックスをオンにします。

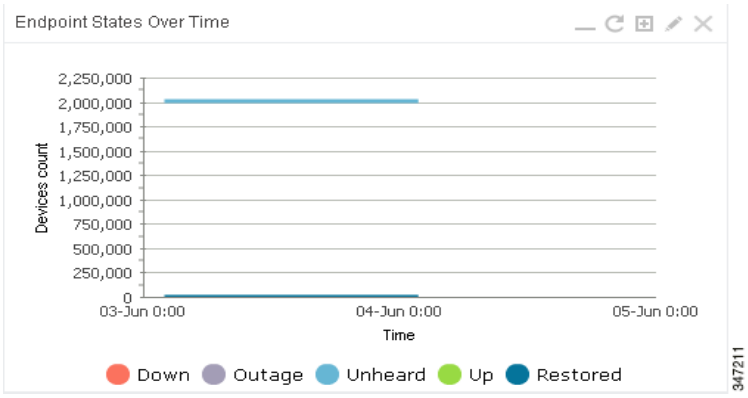
3. [Close] をクリックします。

フィルタの使用

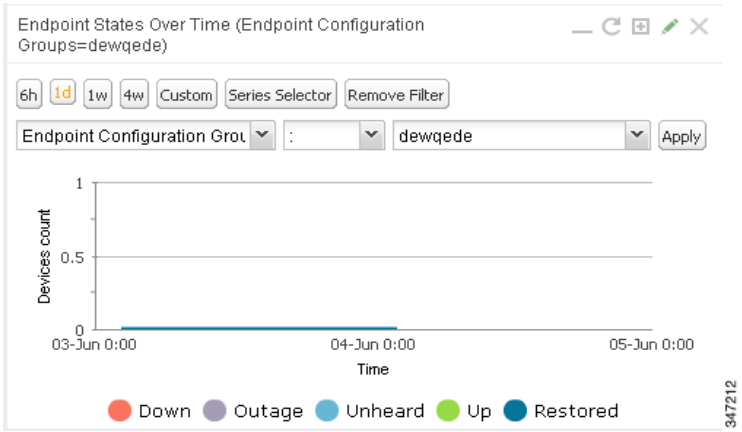
表示されている線グラフをグループ別に表示されるように調整するには、フィルタを使用します。適用されたフィルタが、ダッシュレットのタイトルの後に表示されます。

フィルタを使用するには、次のようにします。

1. 線グラフ ダッシュレット ペインの [Add Filter] をクリックします。



2. 最初のドロップダウン メニューから、グループ タイプを選択します。



3. 3 番目のドロップダウン メニューから、グループを選択します。

4. [Apply] をクリックします。

鉛筆型アイコンは緑色であり、フィルタはそれが適用されるダッシュレット名の横に表示されます。

(注) [Remove Filter] ボタンをクリックし、フィルタを削除して、フィルタ オプションを閉じます。

ダッシュレット データのエクスポート

ダッシュレット データは .csv ファイルにエクスポートできます。

ダッシュレット データをエクスポートするには、次の手順を実行します。

1. 目的のダッシュレットで、エクスポート ボタン( )をクリックします。

   ブラウザのダウンロード セッションが開始されます。

2. デフォルトのダウンロード ディレクトリに移動して、エクスポート ファイルを表示します。

   このファイル名は、先頭が語「export-」であり、ダッシュレット名が含まれます(たとえば、export-Node_State_Over_Time_chart-1392746225010.csv)。

イベントのモニタリング

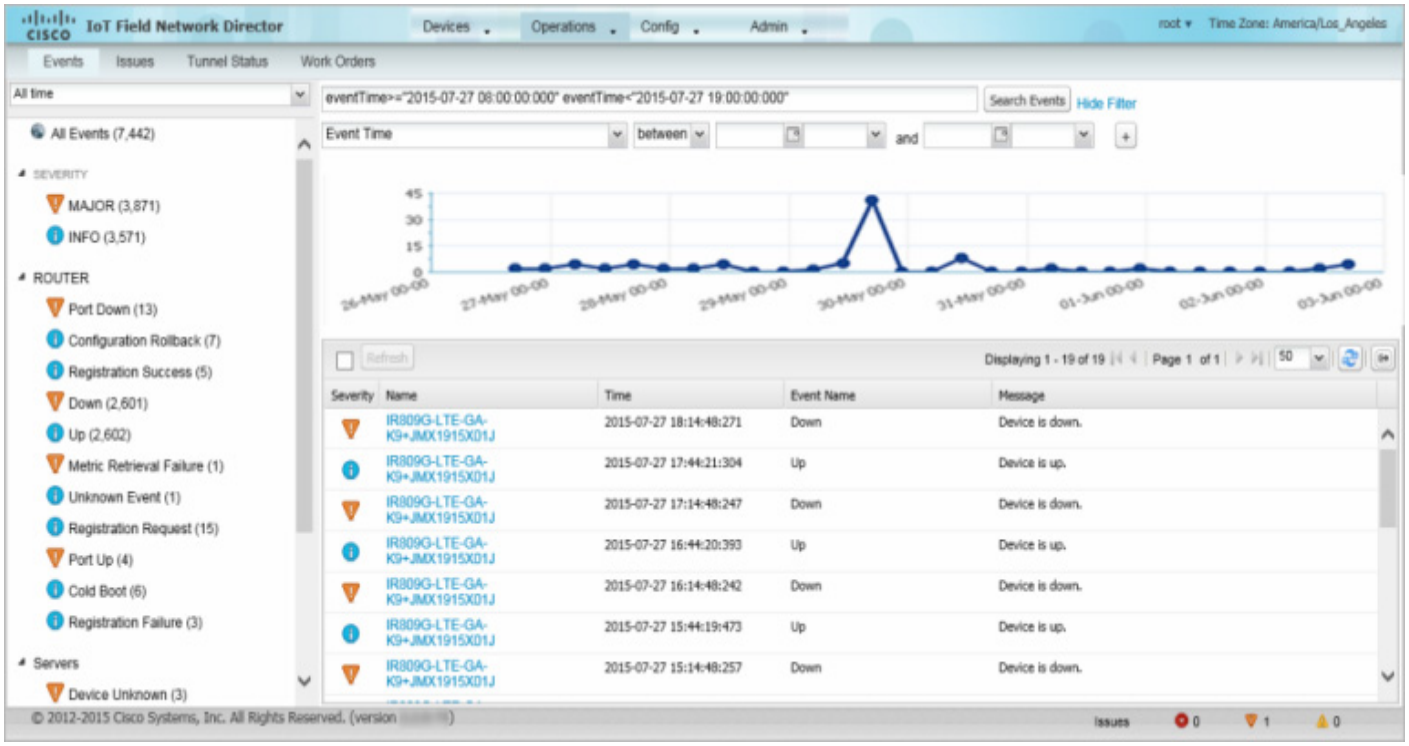
この項では、イベントの概要と、イベントの検索およびソートの方法を説明します。次の内容について説明します。

- イベントの表示
- 重大度レベル別のフィルタリング
- 高度なイベント検索
- イベントのソート
- イベント名での検索
- ラベルによる検索

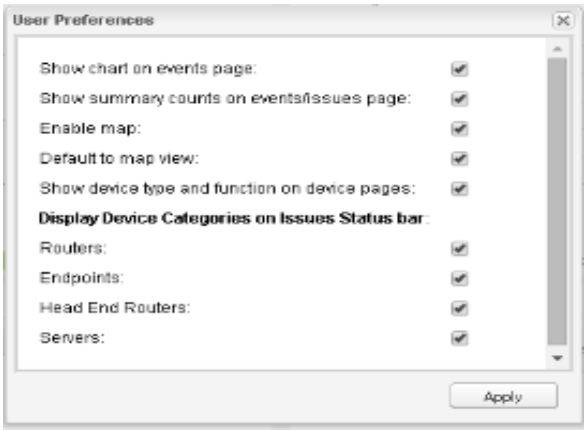
イベントの表示

図 3 に示すように、[Events] ページ([Operations] > [Events])には、IoT FND が追跡するデバイスのすべてのイベントがリストされます。すべてのイベントは、CG-NMS データベース サーバに保存されます。

図 3　[Events] ページ



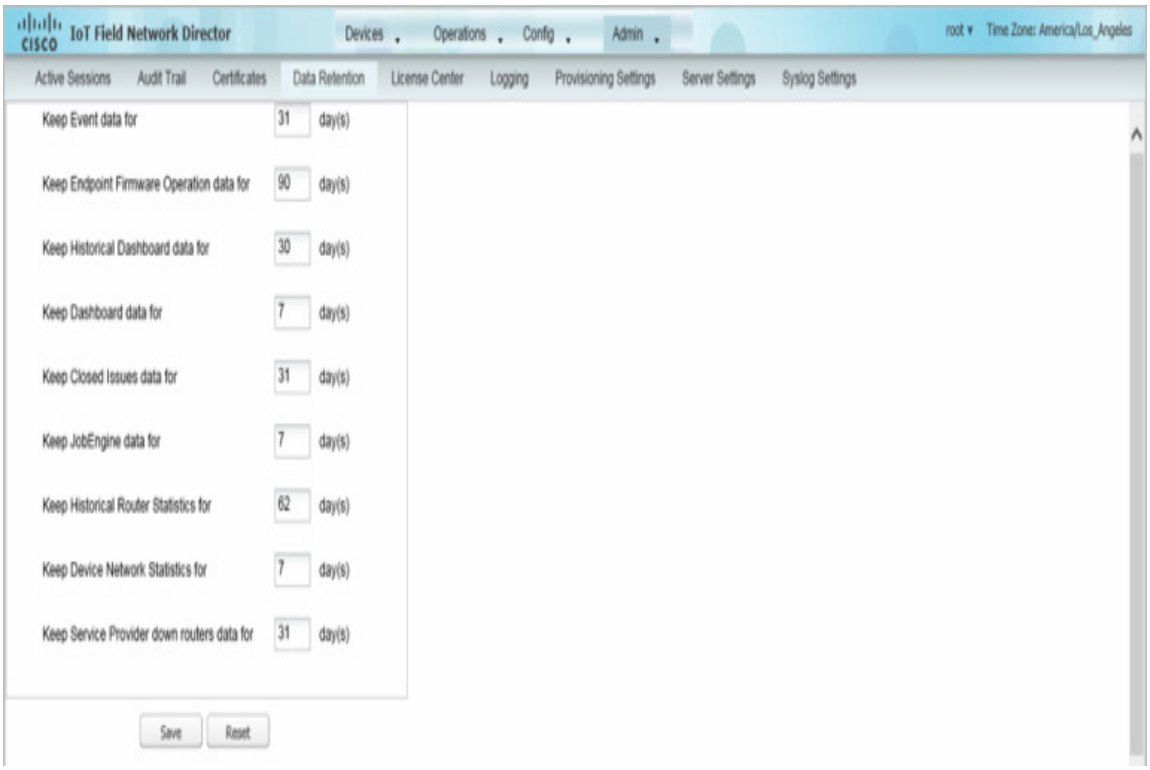
デフォルトでは、[Events] ページには、時系列でのイベントのビジュアル表示であるイベント グラフが表示されます。ただし、CG-NMS サーバが管理するデバイス数によっては、このページはタイムアウトする可能性があります（特にシステムの負荷が限界に達している場合）。その場合、[Preferences] ウィンドウを、[***username***] > [Preferences]（右上）を選択して開き、[Events] ページのグラフと要約カウントの表示のためのチェックボックスをオフにし、[Apply] をクリックします。



このページに表示されるイベント データの量を制限するには、[Filter] ドロップダウン メニュー（左側ペインの上部）を使用します。たとえば、過去 24 時間のイベントを過去 30 日と比較して表示したり、過去の 7 日間のうちの特定の日のイベントを表示したりできます。

イベント データが 14 秒ごとに更新されるように自動更新を有効にするには、[Refresh] ボタンの横のチェック ボックスをオンにします。イベント データを即時に更新するには、[Refresh] ボタンまたは更新アイコンをクリックします。

(注) [Events] ページに表示されるイベント データの量は、イベントのデータ保持設定により制限されます（[Admin] > [System Management] > [Data Retention]）。



[All Events] ペインのフィルタ

イベント タイプのみを表示するには、[All Events] ペインでプリセット フィルタを使用します。

Device Events

左側ペインで、IoT FND は次のデバイスのイベントを追跡します。

- ルータ
- エンドポイント
- ヘッドエンド デバイス
- CG メッシュ デバイス
- NMS サーバ
- データベース サーバ

イベントの重大度レベル

左側ペインで、特定の重大度レベルのデバイスが表示されるようにリスト ビューをフィルタリングするには、イベント重大度レベルを選択します。

- Critical
- Major
- Minor
- Info

各イベント タイプには、プリセットの重大度レベルがあります。たとえば、Router Down イベントは、Major 重大度レベルのイベントです。

デバイス別のプリセット イベント

IoT FND には、追跡する各デバイスの報告に使用する、イベントのプリセット リストがあります。これらのイベントのリストは、[Events] ページの左側ペインに示される各デバイスの下にまとめられています。たとえば、左側ペインで、[Routers] の横の表示/非表示アイコン( )をクリックすると、ルータのすべてのイベントのリストが展開されます。

重大度レベル別のフィルタリング

重大度レベルでフィルタリングするには、次の手順を実行します。

1. [Operations] > [Events] を選択します。
2. [SEVERITY] 表示/非表示矢印をクリックします。

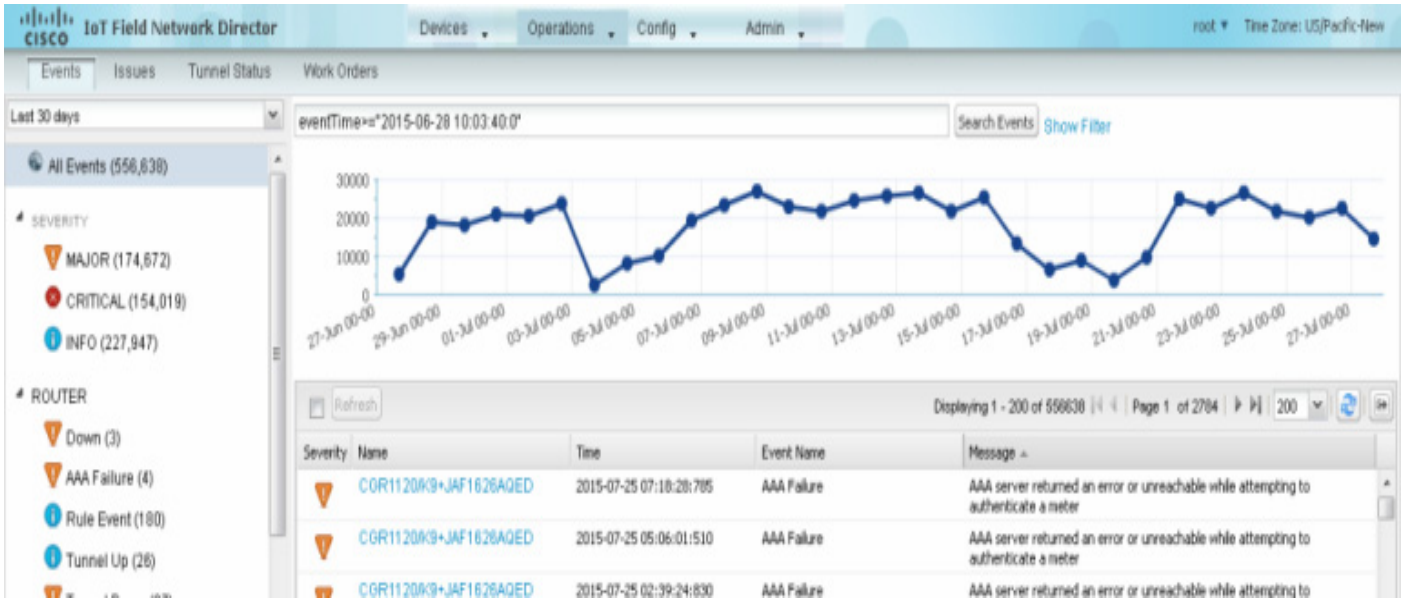
   (注) 表示されるのは発生した重大度レベルのみです。
3. 重大度レベル([CRITICAL]、[MAJOR]、[MINOR]、または [INFO]) をクリックします。

その重大度レベルのすべてのイベントが、[Events] ペインに表示されます。

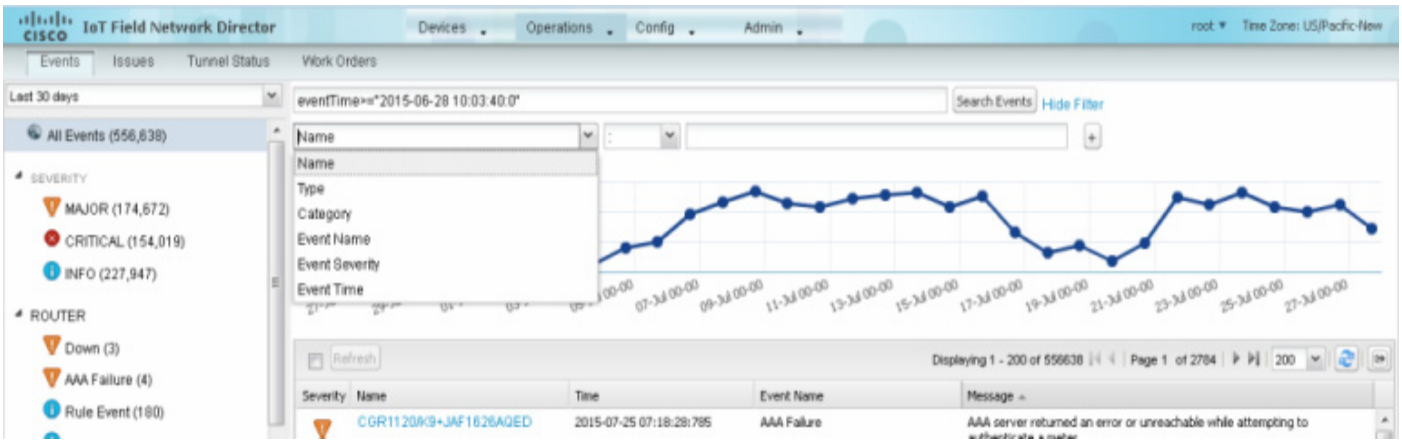
高度なイベント検索

イベントの検索にフィルタを使用するには、次の手順に従います。

1. [Operations] > [Events] を選択します。
2. [All Events](左側ペイン) の下で、イベント カテゴリを選択して検索を絞り込みます。
3. 主要ペインの上部にある [Show Filter] リンクをクリックします。



4. フィルタ ドロップダウン メニューとフィールドを使用して、検索基準を指定します。



5. 正符号ボタン(+)をクリックして、検索文字列を [Search] フィールドに追加します。

   必要に応じて、検索文字列を [Search] フィールドに追加するプロセスを繰り返します。

6. [Search Events] をクリックするか、または Enter を押します。

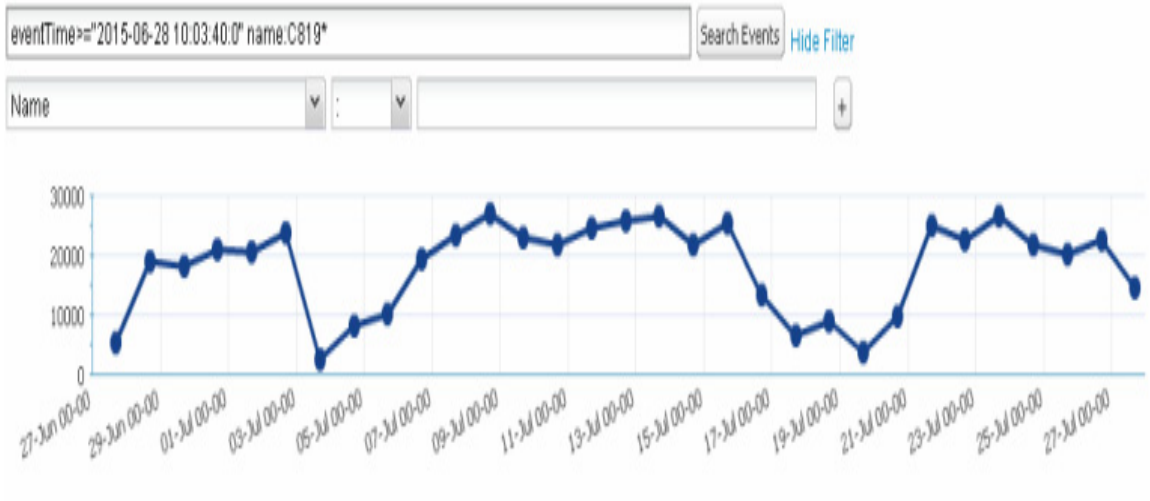
   [Events] ペインに、検索結果が表示されます。

   次の例に示すように、検索文字列を手動で追加することもできます。

   - イベントを名前(EID)でフィルタリングするには、次の文字列を [Search Events] フィールドに入力します。これは 図 3 に示します。

     Name: *router eid string*.

     名前別イベント検索フィルタ



     (注) このフィルタでのアスタリスク(*)ワイルド カードの使用に注意してください。

   - イベントの時間帯でフィルタリングするには、次の文字列を [Search Events] フィールドに入力します。これは 図 4 に示します。

     eventTime*operator*“*YYYY-MM-DD HH:MM:SS:SSS*”

     サポートされる演算子は、<、>、>=、<=、: です。

(注) **eventTime** と演算子の間にはスペースを入力しないでください。

図 4　　時間によるイベント検索フィルタの例

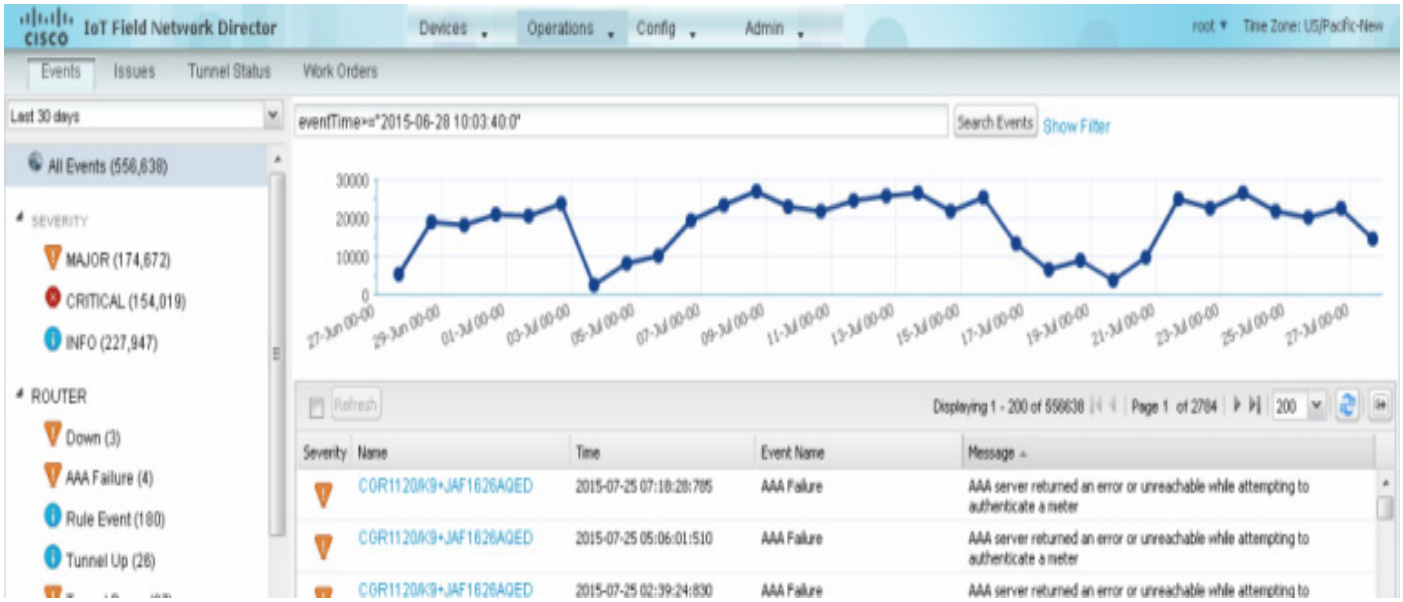
イベントのソート

イベントを昇順または降順でソートするには、任意のカラムにマウス オーバーし、見出しドロップダウン メニューから該当するオプションを選択します。

イベント名での検索

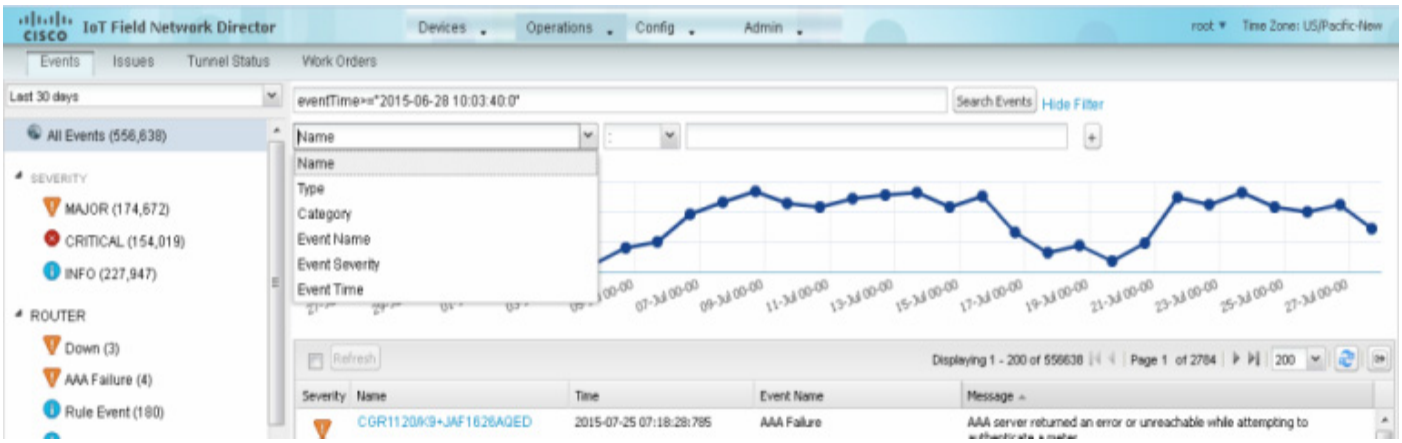
イベント名（たとえば、バッテリ残量低下）で検索するには、次のようにします。

1. [Operations] > [Events] を選択します。
2. 左側ペインで、検索するデバイス タイプをクリックします。
3. 右ペインの上部の [Show Filter] リンクをクリックします。

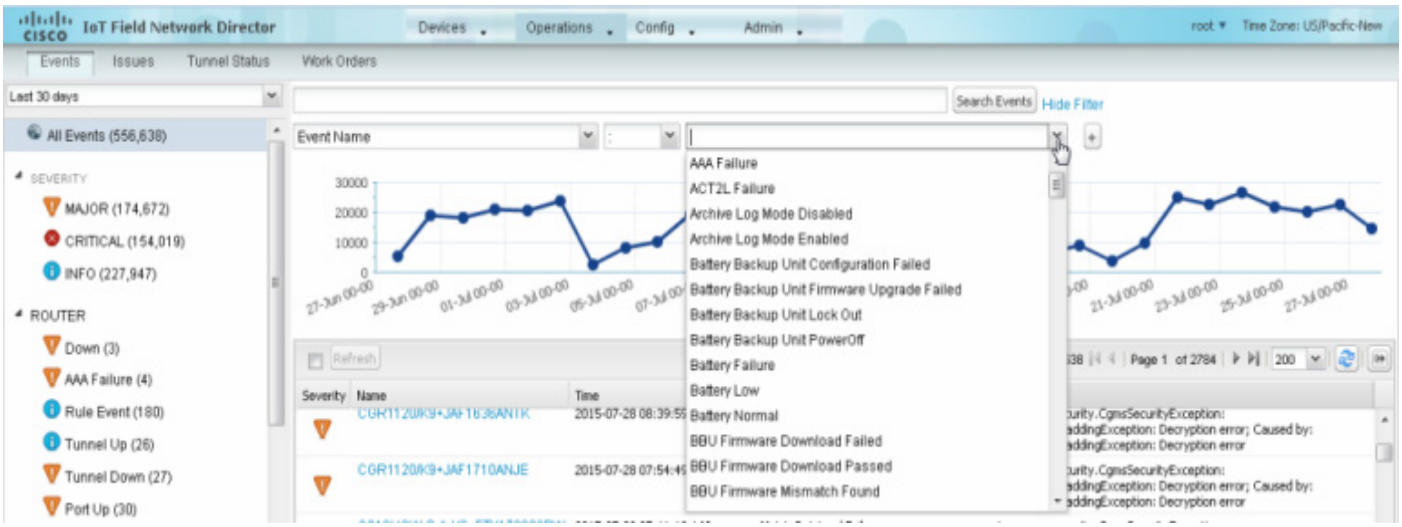


[Search Events] フィールドの下に、フィルタ フィールドが表示されます。

4. 左側のドロップダウン メニューから、[Event Name] を選択します。



5. 右側のドロップダウン メニューの選択肢からイベント名を選択します。



6. 右側の正符号ボタン(+)をクリックして、フィルタを [Search Events] フィールドに追加します。

   フィルタ構文が [Search Events] フィールドに表示されます。

7. [Search Events] ボタンをクリックします。

   [Events] ペインに、検索結果が表示されます。

ラベルによる検索

[Field Devices] にタグ付けされたラベル名に基づいて、イベントを検索およびフィルタリングできます。

1. [Operations] > [Events] を選択します。
2. 左ペインで、[All Events] をクリックします。
3. 右ペインの上部の [Show Filter] リンクをクリックします。
4. 左側のドロップダウン メニューから、[Label] を選択します。
5. 右ペインの上部の [Show Filter] リンクをクリックします。

6. 右側のドロップダウン メニューの選択肢からイベント名を選択するか、または独自に作成します。
7. 右側の正符号ボタン( )をクリックして、フィルタを [Search Events] フィールドに追加します。

   フィルタ構文が [Search Events] フィールドに表示されます。
8. [Search Events] ボタンをクリックします。

   [Events] ペインに、検索結果が表示されます。

イベントのエクスポート

イベントを CSV ファイルにエクスポートして、イベントの重大度、時間、名前、およびイベント説明のデバイスごとのログとして調べることができます。

イベントをエクスポートするには、次の手順を実行します。

1. [Operations] > [Events] を選択します。
2. 左側ペインで、目的の重大度レベルまたはデバイス タイプをクリックします。
3. [Export] ボタン( )をクリックします。

   ブラウザのダウンロード セッションが開始されます。
4. デフォルトのダウンロード ディレクトリに移動して、CSV ファイルにアクセスします。

報告されたイベント

表 1 は、IoT FND 3.1.x 以降で報告されたイベントをリストしています。詳細には、イベント重大度（Critical、Major、Minor、Information）およびそれらのイベントが報告されたデバイスが含まれます。

表 1　　報告されたイベント

イベント	デバイス	重大度
CRITICAL イベント		
証明書が失効	AP800、CGR1000、C800、FND、IR800	Critical
DB FRA Space Critically Low	データベース	Critical
DB Table Space Critically Low	データベース	Critical
Invalid CSMP Signature	CGMESH、IR500	Critical
Outage	セルラー、CGMESH、IR500	Critical
RPL Tree Size Critical	CGR1000	Critical
SD Card Removal Alarm	CGR1000	Critical
MAJOR イベント		
AAA Failure	C800、CGR1000、IR800	Major
ACT2L Failure	C800、CGR1000、IR800	Major
Archive Log Mode Disabled	データベース	Major
Battery Failure	CGR1000	Major
Battery Low	CGR1000、IR500	Major
BBU Configuration Failed	IR500	Major

表 1　報告されたイベント（続き）

イベント	デバイス	重大度
BBU Firmware Download Failed	CGR1000	Major
BBU Firmware Mismatch Found	CGR1000	Major
BBU Firmware Upgrade Failed	IR500	Major
BBU Lock Out	IR500	Major
BBU Power Off	IR500	Major
Block Mesh Device Operation Failed	CGR1000	Major
Certificate Expiration	AP800、C800、CGR1000、FND、IR800	Major
DB FRA Space Very Low	データベース	Major
Default Route Lost	CGMESH、IR500	Major
Device Unknown	FND	Major
Door Open	C800、CGR1000、IR800、LORA	Major
Dot1X Authentication Failure	CGR1000	Major
Dot1X Authentication Flood	C800、CGR1000、IR800	Major
Down	AP800、ASR、C800、セルラー、CGMESH、CGR1000、データベース、FND、IR500、IR800、ISR3900、LORA	Major
Element Configuration Failed	C800、CGR1000、IR800	Major
High CPU Usage	LORA	Major
High Flash Usage	LORA	Major
High Temperature	LORA	Major
HSM Down	FND	Major
Interface Down	ASR、ISR3900	Major
Linecard Failure	C800、CGR1000、IR800	Major
Line Power Failure	C800、CGR1000、IR800	Major
Link Down	IR500	Major
Low Flash Space	C800、CGR1000、IR800	Major
Low Memory/Memory Low	C800、CGR1000、FND、IR800 LORA（メモリ不足）	Major
Low Temperature	LORA	Major
Mesh Connectivity Lost/ Node Connectivity Lost	CGMESH、IR500	Major
Mesh Link Key Timeout/ Node Link Key Timeout	CGMESH、IR500	Major
Metric Retrieval Failure	ASR、C800、CGR1000、IR800、ISR3900	Major
Modem Temperature Cold Alarm	C800、CGR1000、IR800	Major
Modem Temperature Warm Alarm	C800、CGR1000、IR800	Major
Node Connectivity Lost	CGMESH、IR500	Major
Node Link Key Timeout	CGMESH、IR500	Major
Packet Forwarder Usage High	LORA	Major
Port Down	AP800、C800、CGR1000、IR800	Major
Port Failure	AP800、C800、CGR1000、IR800	Major
Refresh Router Mesh Key Failure	CGR1000	Major

表 1　報告されたイベント（続き）

イベント	デバイス	重大度
RPL Tree Size Warning	CGR1000	Major
Software Crash	C800、CGR1000、IR800	Major
SSM Down	FND	Major
System Software Inconsistent	C800、CGR1000、IR800	Major
Temperature Major Alarm	C800、CGR1000、IR800	Major
Time Mismatch	CGMESH、IR500	Major
Tunnel Down	C800、CGR1000、IR800	Major
Tunnel Provisioning Failure	C800、CGR1000、IR800	Major
Unknown WPAN Change	CGMESH、IR500	Major
MINOR イベント		
DB FRA Space Low	データベース	Minor
Dot1X Re-authentication	CGMESH、IR500	Minor
Temperature Minor Alarm	C800、CGR1000、IR800	Minor
Temperature Low Minor Alarm	C800、CGR1000、IR800	Minor
RPL Tree Reset	CGR1000	Minor
INFORMATION イベント		
Archive Log Mode Enabled	データベース	Information
Battery Normal	CGR1000	Information
Battery Power	CGR1000	Information
BBU Firmware Download Passed	CGR1000	Information
Certificate Expiration Recovery	AP800、C800、CGR1000、FND、IR800	Information
Cold Boot	AP800、C800、CGMESH、CGR1000、IR500、IR800	Information
Configuration is Pushed	FND	Information
設定のロール バック	AP800、C800、CGR1000、IR800	Information
DB FRA Space Normal	データベース	Information
DB Table Space Normal	データベース	Information
Device Added	セルラー、C800、CGMESH、CGR1000、IR500、IR800	Information
Device Location Changed	C800、CGR1000、IR800	Information
Device Removed	セルラー、C800、CGMESH、CGR1000、IR500、IR800	Information
Door Close	C800、CGR1000、IR800、LORA	Information
Dot11 Deauthenticate Send	C800、CGR1000、IR800	Information
Dot11 Disassociate Send	C800、CGR1000、IR800	Information
Dot11 Authentication Failed	C800、CGR1000、IR800	Information
Hardware Insertion	C800、CGR1000、IR800	Information
Hardware Removal	C800、CGR1000、IR800	Information
High CPU Usage Recovery	LORA	Information
High Flash Usage Recovery	LORA	Information
High Temperature Recovery	LORA	Information

表 1　報告されたイベント（続き）

イベント	デバイス	重大度
HSM Up	FND	Information
Interface Up	ASR、ISR3900	Information
Line Power	C800、CGR1000、IR800	Information
Line Power Restored	C800、CGR1000、IR800	Information
Link Up	IR500	Information
Low Flash Space OK	C800、CGR1000、IR800	Information
Low Memory OK/Low Memory Recovery	C800、CGR1000、IR800、LORA（低メモリ リカバリ）	Information
Manual Close	ASR、セルラー、C800、CGMESH、CGR1000、IR500、IR800、ISR3900	Information
Major RPL Tree Size Warning OK	CGR1000	Information
Manual NMS Address Change	CGMESH、IR500	Information
Manual Re-Registration	CGMESH、IR500	Information
Mesh Certificate Change/ Node Certificate Change	CGMESH、IR500	Information
Mesh Module Firmware Upgrade has been successful	CGR1000	Information
Migrated To Better PAN	CGMESH、IR500	Information
Modem Status Changed	LORA	Information
Modem Temperature Cold Alarm Recovery	C800、CGR1000、IR800	Information
Modem Temperature Warm Alarm Recovery	C800、CGR1000、IR800	Information
NMS Address Change	CGMESH、IR500	Information
NMS Returned Error	CGMESH、IR500	Information
Node Certificate Change	CGMESH、IR500	Information
Packet Forwarded High Usage Recovery	LORA	Information
Packet Forwarder Status	LORA	Information
Packet Forwarded High Usage Recovery	LORA	Information
Port Up	AP800、C800、CGR1000、IR800	Information
Power Source OK	C800、CGR1000、IR800	Information
Power Source Warning	C800、CGR1000、IR800	Information
Registered	ASR、ISR3900	Information
登録失敗	AP800、Cellular、C800、CGR1000、IR800、LORA	Information
登録要求	AP800、C800、CGR1000、IR800、LORA	Information
登録成功	AP800、Cellular、C800、CGR1000、IR800、LORA	Information
Rejoined With New IP Address	CGMESH、IR500	Information
Restoration	セルラー、CGMESH、IR500	Information
Restoration Registration	CGMESH、IR500	Information
RPL Tree Size Critical OK	CGR1000	Information

表 1　報告されたイベント（続き）

イベント	デバイス	重大度
ルール イベント	ASR、C800、CGMESH、CGR1000、データベース、FND、IR500、IR800、ISR3900	Information
SSM Up	FND	Information
Temperature Low Recovery	LORA	Information
Temperature Low Minor Alarm Recovery	C800、CGR1000、IR800	Information
Temperature Major Recovery	C800、CGR1000、IR800	Information
Temperature Low Major Alarm Recovery	C800、CGR1000、IR800	Information
Temperature Minor Recovery	C800、CGR1000、IR800	Information
Time Mismatch Resolved	CGMESH、IR500	Information
Tunnel Provisioning Request	C800、CGR1000、IR800	Information
Tunnel Provisioning Success	C800、CGR1000、IR800	Information
Tunnel Up	C800、CGR1000、IR800	Information
Unknown Event	AP800、ASR、C800、セルラー、CGMESH、CGR1000、データベース、FND、IR500、IR800、ISR3900、LORA	Information
Unknown Registration Reason	CGMESH、IR500	Information
Unsupported	AP800、C800、CGR1000、IR800、LORA	Information
Up	AP800、ASR、C800、セルラー、CGMESH、CGR1000、データベース、FND、IR500、IR800、ISR3900、LORA	Information
Warm Start	IR500	Information
WPAN Watchdog Reload	CGR1000	Information

モニタリングの問題

この項では、IoT FND の問題の概要と、問題の検索およびクローズの方法を説明します。次の内容について説明します。

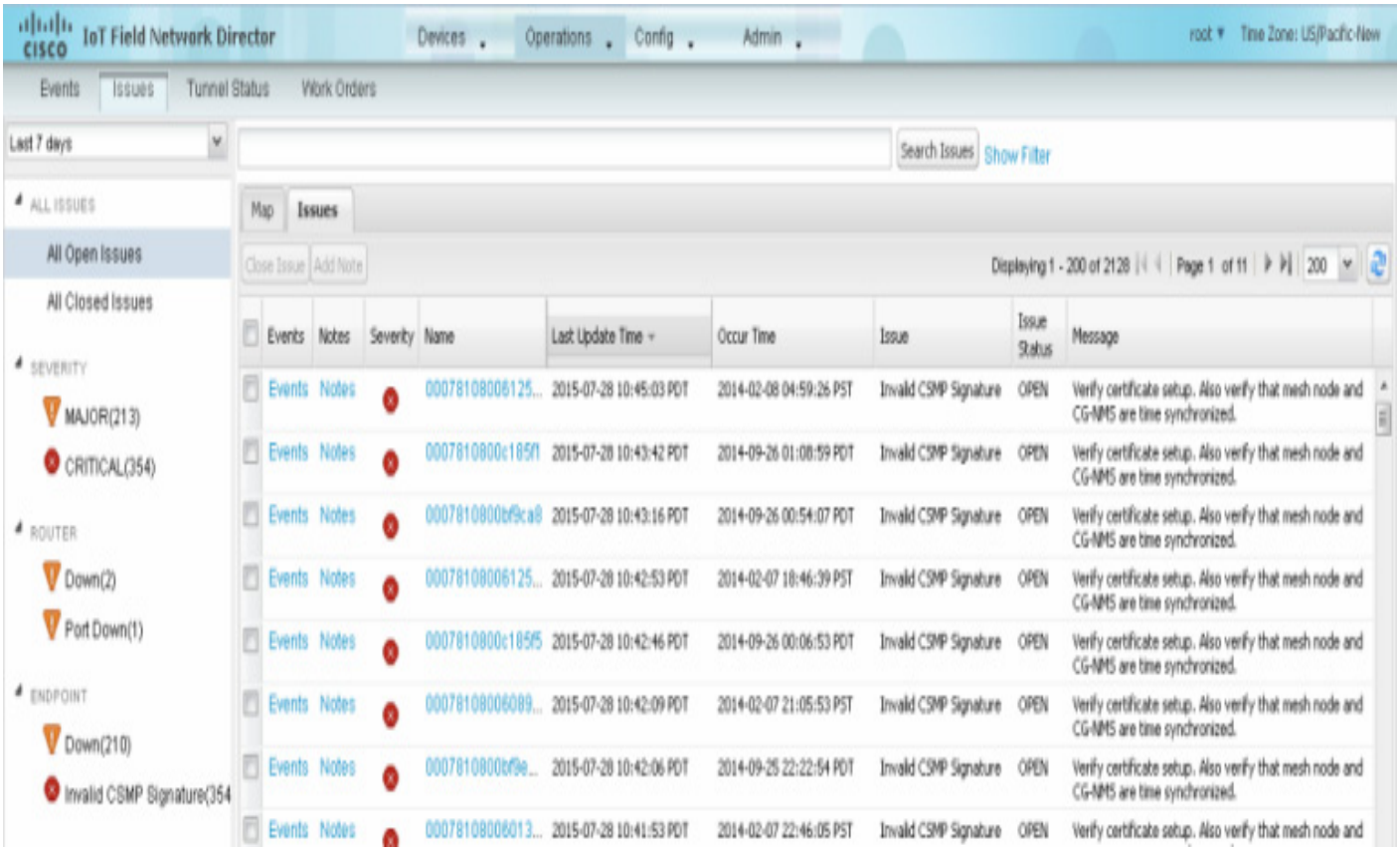
- 問題の表示
- [Issues] ステータス バーでのデバイス重大度ステータスの表示
- 問題へのメモの追加
- 事前定義フィルタを使用した問題の検索
- カスタム フィルタを使用した問題の検索
- 問題のクローズ

問題の表示

IoT FND は、問題をモニタするためのさまざまな方法を提供しています。

- [Operations] > [Issues] ページ（図 5）には、ネットワークのヘルスのスナップショットが表示され、ネットワーク内でアクティブである Major および Critical のイベントのみが強調表示されます。
- [Issues] ステータス バー（図 6）は、ブラウザ ウィンドウのフッターに表示され、選択したデバイスについて重大度別にすべての問題数を示します。

図 5　[Issues] ページ



[Issues] ページには、管理者によるクイック レビューと解決のために、未解決のネットワーク イベントの簡易サブセットが表示されます。問題は、関連イベントが解決される（そして IoT FND が解決イベントを生成する）か、または管理者が手動でイベントを閉じるかのいずれかまでは、未解決のままです。

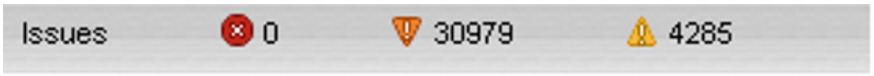
同じイベントについて複数の項目が報告される場合は、1 つの問題のみが記録されます。各問題には、それに関連付けられたカウンタがあります。関連イベントがクローズされると、カウンタは 1 だけ減分されます。未解決のまたはクローズされたすべての問題には、関連イベントがあります。

(注) [Issues] ページに表示されるクローズされた問題データの量は、[Keep Closed Issues for] データ保持設定（[Admin] > [System Management] > [Data Retention]）により制限されます。これは問題がクローズされた時刻に基づいて決まります。問題が閉じられた時刻は、その問題の [Last Update Time] として表示されます。

[Issues] ステータス バーでのデバイス重大度ステータスの表示

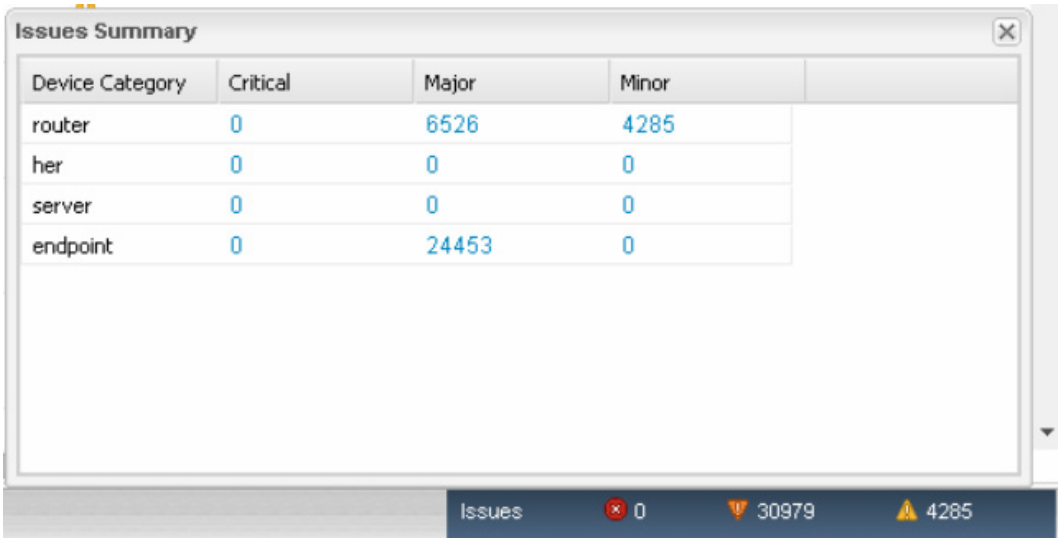
選択したデバイスについて重大度別にリストされた問題の集計は、ブラウザ ウィンドウ フレームの右下にある [Issues] ステータス バーに表示されます（図 6）。[User Preferences] の [Issues] ステータス バーに表示される問題に対して、デバイス タイプを設定できます（ユーザ プリファレンスの設定を参照）。

図 6　[Issues] ステータス バー



[Issues] ステータス バーをクリックすると、[Issues Summary] ペインが表示されます（図 7）。それには、選択したデバイス カテゴリ別にリストされた問題が表示されます。[Issues Summary] ペインのカウント リンクをクリックすると、[Operations] > [Issues] ページに、重大度でフィルタリングされた詳細な問題の基準が表示されます。

図 7　[Issues Summary] ペイン

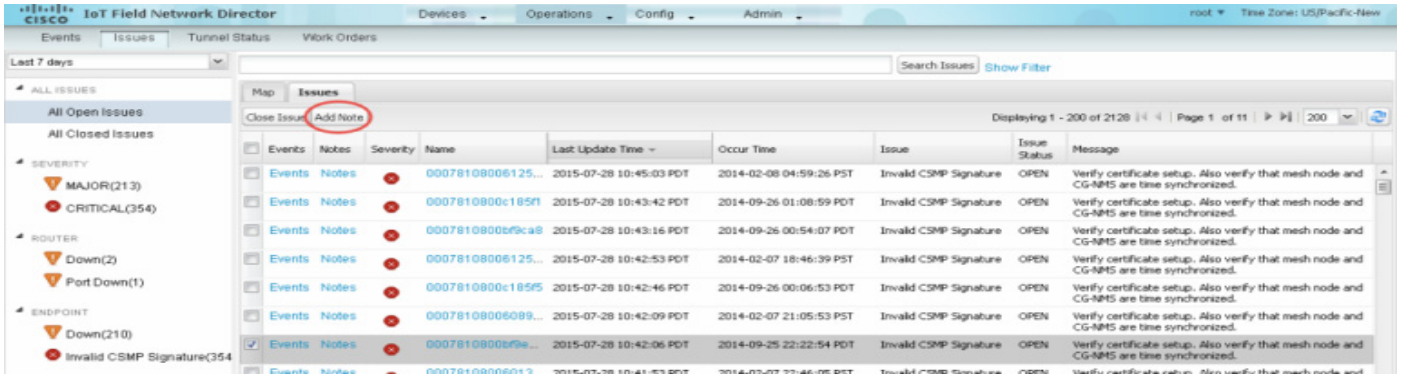


問題へのメモの追加

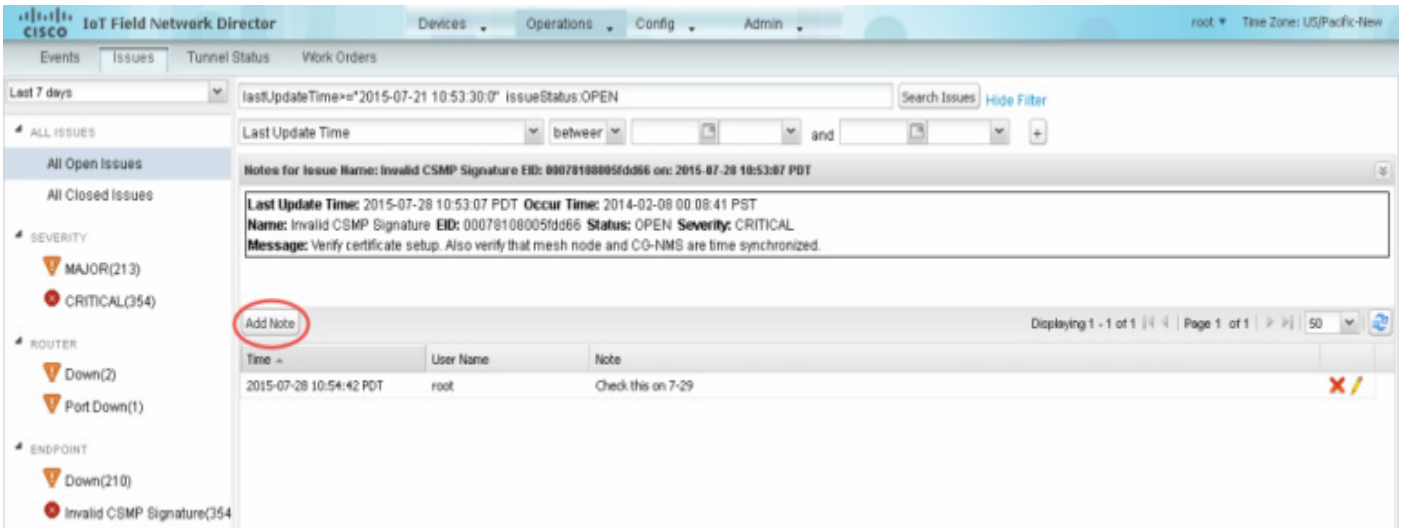
[Operations] > [Issues] ページで、デバイスの問題に関するメモを保持できます。問題に入力されているメモにアクセスしたり、[Notes for Issues Name] ページでメモを追加したりするには、問題に埋め込まれている [Notes] リンクをクリックします。このページ上で、メモを編集したり問題からメモを削除したりできます。問題には複数のメモを追加できます。[Notes for Issues Name] ページには、メモが作成された時刻、メモを作成したユーザの名前、およびメモのテキストが表示されます。問題をクローズするときに、メモを追加することもできます。メモは問題と共にデータベースから消去されます。

メモを問題に追加するには、次の手順を実行します。

1. 目的とする問題に埋め込まれている [Notes] リンクをクリックするか、またはデバイスのチェックボックスをオンにして、[Add Note] をクリックします。

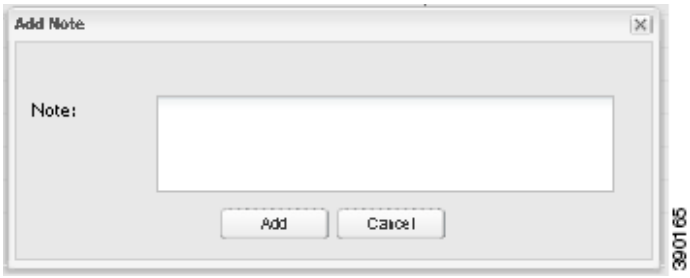


[Notes for Issues Name] ペインが表示されます。次に示す例では、問題には既存のメモがあります。



2. [Add Note] をクリックします。

   [Add Note] ダイアログが表示されます。



3. カーソルを [Note] フィールドに置いて、メモを入力します。
4. 終了したら、[Add] をクリックします。

メモのテキストが、[Note] カラムの [Notes for Issues Name] ペインに表示されます。

既存のメモがある問題にメモを追加するには、次の手順を実行します。

1. 問題に埋め込まれている [Notes] リンクをクリックするか、またはデバイスのチェックボックスをオンにして、[Add Note] をクリックします。

   [Notes for Issues Name] ペインが表示されます。

2. 問題に新しいメモを追加するには、[Add Note] をクリックします。

   [Add Note] ダイアログが表示されます。

3. カーソルを [Note] フィールドに置いて、メモを入力します。
4. 終了したら、[Add] をクリックします。

問題の既存のメモを編集するには、次の手順を実行します。

1. 問題に埋め込まれている [Notes] リンクをクリックします。

   [Notes for Issues Name] ペインが表示されます。

2. 既存のメモを編集するには、編集するメモの右側にある鉛筆型アイコン( )をクリックします。

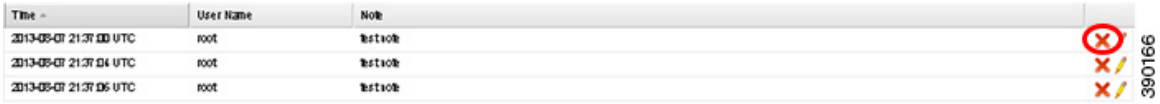
3. メモを編集し、終了したら [Done] をクリックします。

問題からメモを削除するには、次の手順を実行します。

1. 問題に埋め込まれている [Notes] リンクをクリックします。

   [Notes for Issues Name] ペインが表示されます。

2. メモを削除するには、メモの右側にある赤い X アイコン（ ）をクリックします。

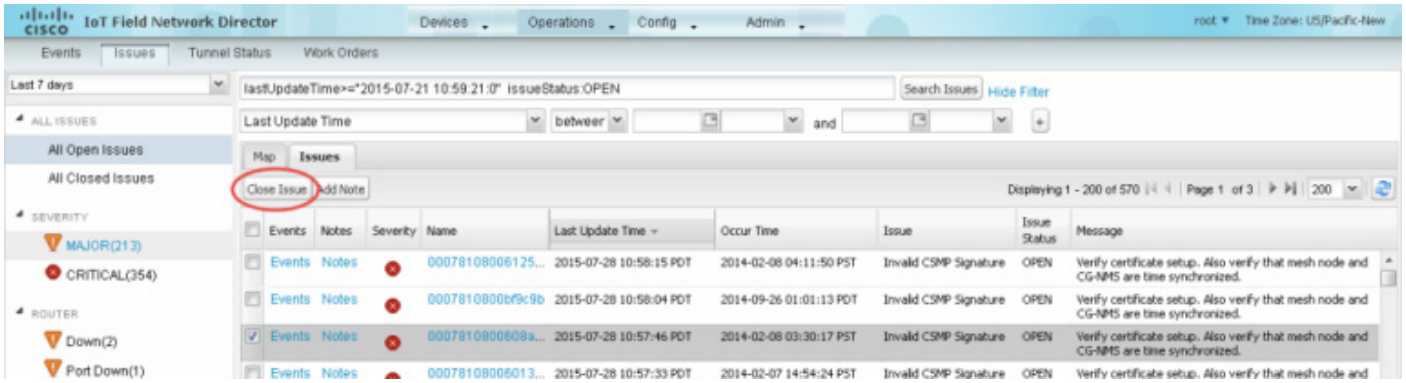


3. [Yes] をクリックして削除を確定します。

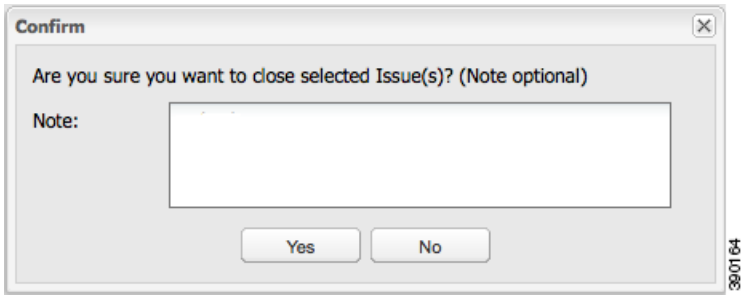
問題を閉じるときにメモを追加するには、次の手順を実行します。

1. 閉じる問題のチェックボックスをオンにします。

2. [Close Issue] をクリックします。



3. [Confirm] ダイアログ ボックスで、カーソルを [Note] フィールドに挿入して、メモのテキストを入力します。



4. 問題を閉じてメモを保存することを確定するには、[Yes] をクリックします。

事前定義フィルタを使用した問題の検索

特定のシステムまたは重大度レベルの未解決問題を検索するには、次の手順を実行します。

1. [Operations] > [Issues] を選択します。

   未解決の問題のみをリストするには、[All Open Issues] をクリックします(左側ペイン)。

   (注)デフォルトでは、IoT FND は、指定のデータ保持期間内に発生したすべての問題を表示します(データ保存の設定を参照)。イベント タイプまたは重大度レベルに関連付けられているクローズした問題を表示するには、[Search Issues] フィールドで **issueStatus:OPEN** を **issueStatus:CLOSED** に変更し、[Search Issues] をクリックします。クローズしたすべての問題をリストするには、左側ペインで [All Closed Issues] をクリックします。

2. デバイス カテゴリ、イベント タイプ、または重大度をクリックして、リストをフィルタリングします。

フィルタ構文は [Search Issues] フィールドに表示され、検索結果はメイン ペインに表示されます。

カスタム フィルタを使用した問題の検索

カスタム フィルタを作成して検索するには、次の手順を実行します。

1. [Operations] > [Issues] を選択します。
2. [Show Filter] をクリックします。
3. [Filter] ドロップダウン メニューから、適切なオプションを選択します。

   たとえば、重大度レベルを EID でフィルタリングするには、次の手順を実行します。

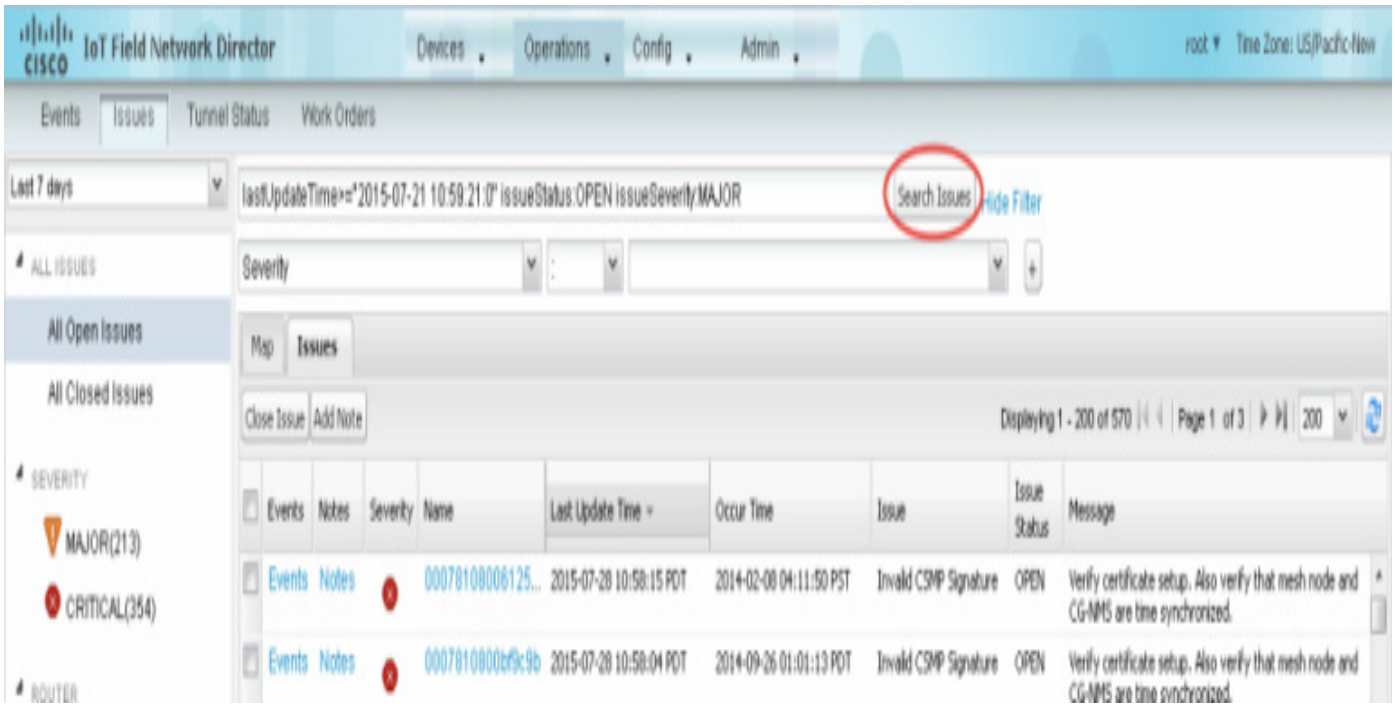
   - 左ペインで、重大度レベルを選択します。
   - 最初の [Filter] ドロップダウン メニューから、[EID] を選択します。
   - 3 番目の [Filter] フィールドには、問題の検出対象デバイスの EID を入力します。

   [Search Issues] フィールドに検索文字列を入力することもできます。次に例を示します。

   issueSeverity:CRITICAL issueStatus:OPEN eid:CG-NMS-DB+localhost

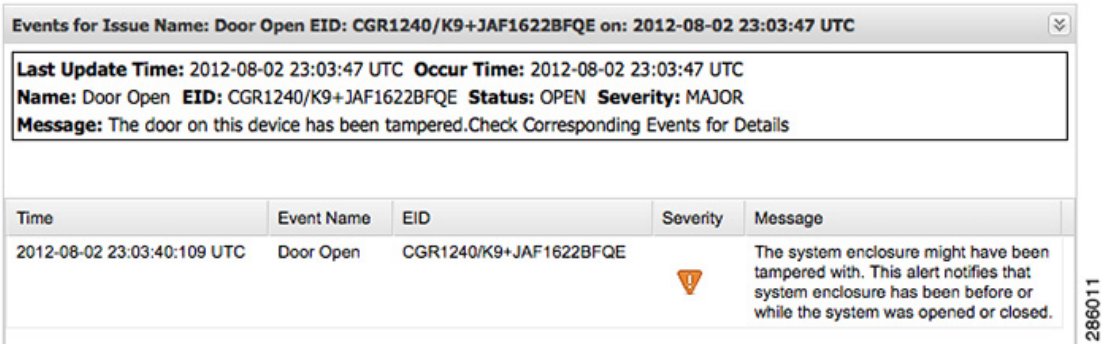
4. [Search Issues] をクリックします。

   問題があれば、[Search Issues] セクション(右側ペイン)に表示されます。



5. [Events] リンクをクリックして、問題に関連するイベントを表示します。

   [Events for Issue Name] ペインに、そのデバイスのすべてのイベントが表示されます。



6. [Search Issues] または左側ペインの任意のリンクをクリックすると、[Issues] ペインに戻ります。

問題のクローズ

たいていの場合、イベントが解決されると、問題はソフトウェアにより自動的にクローズされます。ただし、管理者が問題の解決をアクティブに行ったときは、問題を直接クローズすることに意味がある場合があります。問題がクローズしても、IoT FND はイベントを生成します。

解決した問題をクローズするには、次の手順を実行します。

1. [Operations] > [Issues] を選択します。
2. 事前定義フィルタを使用した問題の検索またはカスタム フィルタを使用した問題の検索のいずれかの項に記載されている手順に従って問題を特定します。

3. [Search Issues] セクション(右側ペイン)で、クローズする問題のチェックボックスをオンにします。
4. [Close Issue] をクリックします。

   (注) この時点で問題にメモを追加することもできます。
5. [Yes] をクリックします。

デバイス グラフの表示

- ルータ チャート
- メッシュ エンドポイント グラフ

ルータ チャート

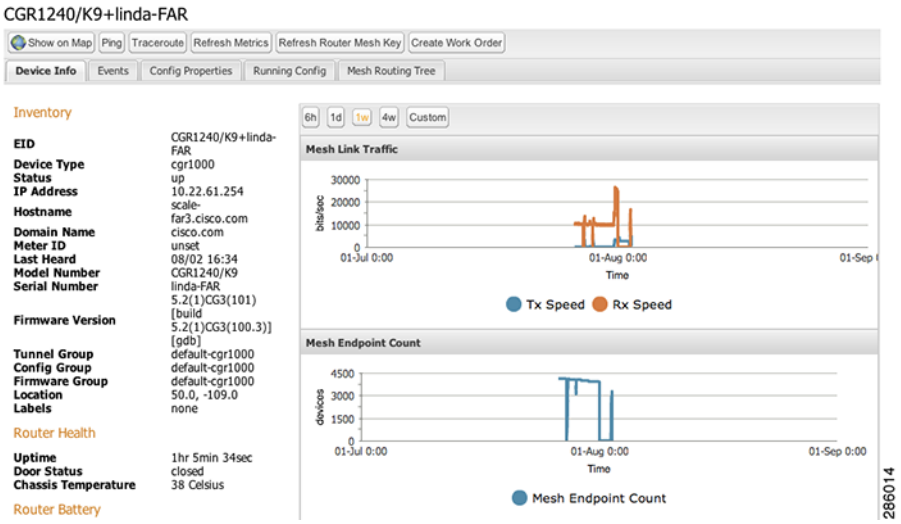
IoT FND は、すべての FAR について、[Device Details] ページの [Device Info] ペインにこれらのグラフを表示します。

表 2　デバイス詳細のグラフ

グラフ	説明
Mesh Link Traffic	時間の経過に応じた FAR の集約 WPAN レートを示します。
Mesh Endpoint Count	時間の経過に応じた ME 数を示します。
Cellular Link Metrics	すべての論理セルラー GSM および CDMA インターフェイスのメトリック(送信および受信速度)、RSSI 帯域幅使用率(現在の課金サイクル)を示します。
Cellular Link Settings	デュアルおよびシングル モデムとのセルラー物理インターフェイスのプロパティを示します。
Cellular Link Traffic	時間の経過に応じたプロトコルごとの集約 WPAN レートを示します。
Cellular RSSI	セルラー RSSI。
WiMAX Link Traffic	時間の経過に応じた FAR の WiMAX リンク トラフィックの送受信レートを示します。
WiMAX RSSI	時間の経過に応じた FAR の WiMAX RSSI トラフィックの送受信レートを示します。
WPAN Traffic	(マスターのみ)デュアル PHY WPAN トラフィックのトレンドを示します。
Ethernet Link Traffic	時間の経過に応じた FAR のイーサネット トラフィックの送受信レートを示します。
Cellular Bandwidth Usage Over Time	時間の経過に応じたセルラー インターフェイスの帯域幅の使用を示します。
Ethernet Bandwidth Usage Over Time	時間の経過に応じたイーサネット インターフェイスの帯域幅の使用を示します。

図 8 は、メッシュ リンク トラフィックおよびメッシュ エンドポイント数のグラフを示しています。

図 8　FAR デバイス グラフ



メッシュ エンドポイント グラフ

IoT FND は、すべての ME について、[Device Details] ページの [Device Info] ペインに、表 3 でリストされているグラフを表示します（図 9）。

表 3　デバイス詳細のグラフ

グラフ	説明
Mesh Link Traffic	時間の経過に応じた FAR の集約 WPAN レートを示します。
Mesh Path Cost and Hops	時間の経過に応じた、要素とルーティング ツリーのルートとの間の RPL パス コスト値を表示します（RPL ツリー ポーリングの設定を参照）。
Mesh Link Cost	時間の経過に応じた、要素とそのアップリンク ネイバーとの間のリンクの RPL コスト値を表示します。
Mesh RSSI	時間の経過に応じた、プライマリ メッシュ RF アップリンク（dBm）の測定された RSSI 値を表示します。

図 9　　メッシュ エンドポイント デバイスのグラフ

<< Back

00173BAB003C3100

Show on Map | Ping | Traceroute | Sync Config Membership | Sync Firmware Membership | Block Mesh Device

Device Info | Events | Config Properties | Mesh Routing Tree

Inventory

EID	00173BAB003C3100
Device Type	cgmesh
Status	up
IP Address	2001:dead:beef:6108:217:3bab:3c:3100
Meter ID	unset
Last Heard	2012-07-24 17:05
Model Number	OWCM/3.1
Serial Number	00173BAB003C3100
Firmware Version	5.0.92
Config Group	default-cgmesh
Firmware Group	default-cgmesh
Location	49.4, -132.9
Labels	none

Mesh Endpoint Health

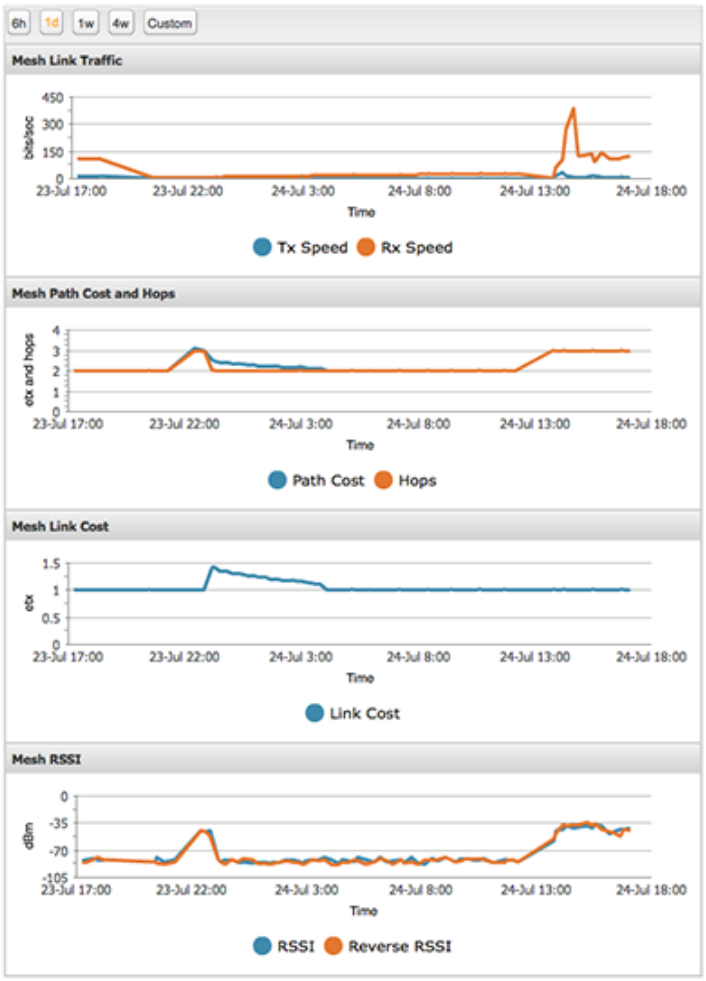
Uptime	unknown

Mesh Link Settings

SSID	unit
PANID	323
Transmit Power	-34
Security Mode	1

Mesh Link Metrics

Mesh Link Transmit Speed	7.32 bits/sec
Mesh Link Receive Speed	121.63 bits/sec
Mesh Link Transmit Packet Drops	0 drops/sec
Mesh Route RPL Hops	3 hops
Mesh Route RPL Link Cost	1
Mesh Route RPL Path Cost	3
Mesh Route RSSI	-42 dBm
Mesh Route Reverse RSSI	-45 dBm



Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bits/sec)	Tx Drops (bits/sec)	Rx Speed (bits/sec)
lo	up	up	0:0:0:0:0:0:0:1/64		0		0
lowpan	up	up	2001:dead:beef:6108:217:3bab:3c:3100/64 fe80:0:0:0:217:3bab:3c:3100/64	00173bab003c3100	6.8		139.55
ppp	up	up	fe80:0:0:0:0:0:0:1/64	00173bab003c3100	13.24		7.43

Network Routes

Destination	Next Hop IP Address	Next Hop Element ID	Interface	Hops	Path Cost	Link Cost	RSSI	Reverse RSSI
default	fe80:0:0:0:217:3bab:3c:3102	00173BAB003C3102	lowpan	3	3	1	-39	-43

Routing Path

Hops	IP Address	Element ID	Status	Last Heard
this element	2001:dead:beef:6108:217:3bab:3c:3100	00173BAB003C3100	up	2012-07-24 17:05
1 hop	2001:dead:beef:6108:217:3bab:3c:3102	00173BAB003C3102	up	2012-07-24 16:44
2 Hops	2001:dead:beef:6108:217:3bab:3c:3208	00173BAB003C3208	up	2012-07-24 16:53

286000

ハイ アベイラビリティのインストールの管理

ここでは、ハイ アベイラビリティ用に IoT FND を設定する方法について説明します。具体的な内容は次のとおりです。

IoT FND ハイ アベイラビリティの概要

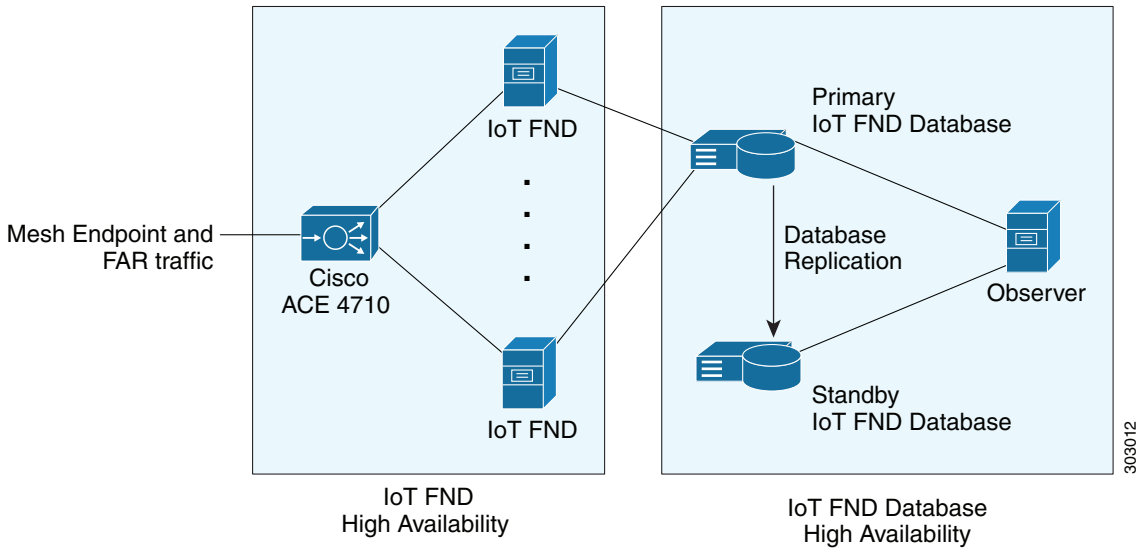
ここでは、IoT FND ハイ アベイラビリティのインストールの概要を提供します。具体的な内容は次のとおりです。

IoT FNDは、Connected Grid のモニタおよび管理にとって重要なアプリケーションです。IoT FND ハイ アベイラビリティ（IoT FND HA）ソリューションは、ソフトウェア、ネットワーク、またはハードウェアの障害発生時に、IoT FND の全体的な可用性に対応します。

図 1 に示すように、IoT FND は 2 つの主要なレベルの HA を提供します。

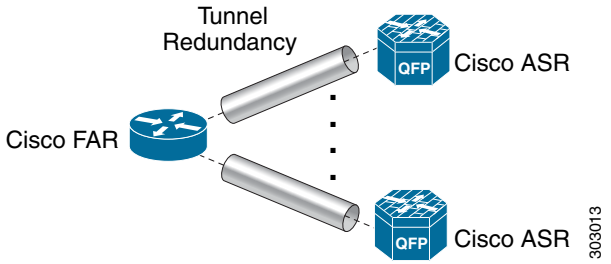
- IoT FND サーバ HA：これは複数の IoT FND サーバを Cisco ACE 4710 ロード バランサに接続することで実現されます。ME、FAR、ASR で発生するトラフィックは、ロード バランサに送られます。ロード バランサは、ラウンドロビン プロトコルを使用して IoT FND クラスタ サーバ間で負荷を分散します。
- IoT FND データベース HA：これは 2 つの IoT FND データベース サーバ（プライマリ サーバとスタンバイ（セカンダリ）サーバ）を設定することで実現されます。プライマリ データベースは新しいデータを受信すると、コピーをスタンバイ データベースに送信します。別のシステムがオブザーバを実行します。オブザーバは IoT FND データベース サーバをモニタするプログラムで、スタンバイ サーバでも実行できます。プライマリ データベースに障害が発生すると、オブザーバはスタンバイ サーバを新しいプライマリ データベースとして設定します。IoT FND データベース HA は、シングルおよびクラスタ IoT FND サーバ展開でも機能します。

図 1　IoT FND サーバおよびデータベース HA



IoT FND サーバとデータベース HA に加え、トンネルの冗長性を加えることで IoT FND の信頼性が向上します。これは 1 つの FAR と複数の ASR 間で複数のトンネルを定義することで実現されます。1 つのトンネルで障害が発生すると、FAR は別のトンネル経由でトラフィックをルーティングします。

図 2　IoT FND トンネルの冗長性



IoT FND HA は、以下の障害シナリオに対応します。

障害のタイプ	説明
IoT FND サーバの障害	IoT FND サーバ クラスタ内の 1 台のサーバに障害が発生すると、ロード バランサがクラスタ内の他のサーバにトラフィックをルーティングします。
IoT FND データベースの障害	プライマリ データベースに障害が発生すると、関連付けられたスタンバイ データベースがプライマリ データベースになります。これは IoT FND サーバに対してトランスペアレントです。クラスタ内のすべての IoT FND サーバが新しいプライマリ データベースに接続します。
トンネルの障害	トンネルに障害が発生すると、トラフィック フローは別のトンネルを経由します。

ロード バランサ

ロード バランサ（LB）は以下のタスクを実行するため、IoT FND HA において重要な役割を担います。

- IoT FND へのトラフィックを負荷分散します。
- クラスタ内のサーバとのハートビートを維持し、障害を検出します。IoT FND サーバに障害が発生すると、LB は他のクラスタ メンバーにトラフィックを向けます。

この展開では、ロード バランサとして Cisco ACE 4710（Cisco ACE）を使用することを推奨します。Cisco ACE 4710 の詳細については、http://www.cisco.com/en/US/partner/products/ps7027/tsd_products_support_series_home.html を参照してください。

サーバのハートビート

LB は、クラスタ内の各 IoT FND サーバとのハートビートを維持します。IoT FND ソリューション（代替ソリューションあり）で採用されているヘルス モニタリング メカニズムでは、ハートビートはポート 80 での IoT FND への 通常の GET メッセージです。IoT FND はアクティブな IoT FND サーバからの「HTTP 200 OK」の応答を求めます。

LB で次のハートビート パラメータを設定できます。

- Periodicity of probes：これはハートビート間の秒数です。Cisco ACE でのデフォルト値は 15 秒です。
- Number of retries：これは LB が応答しない IoT FND サーバにダウンを宣言する前に、ハートビートの送信を試行する回数です。デフォルトの再試行回数は 3、
- Regular checks after failure detection：LB はこの時間間隔でサーバがオンラインに戻ったかどうかを確認します。障害検出チェックのデフォルト値は 60 秒です。

データベース ハイ アベイラビリティ

IoT FND データベース HA は、IoT FND シングル サーバーとクラスタ展開で機能します。IoT FND HA は Oracle Active Dataguard を使用して、Oracle HA を展開します。IoT FND データベース用に HA を設定するには、Oracle Recovery Manager（RMAN）と Dataguard Management CLI（DGMGRL）を使用します。

IoT FND データベース HA 設定プロセスには以下が含まれます。

- 別の物理サーバでプライマリ データベースとセカンダリ データベースを同じように設定します。

  (注) セカンダリ データベース サーバは、スタンバイ データベースとも呼ばれます。

  (注) データベースのフェールオーバー時に、データが失われる可能性があります。

- Oracle *ウォレット*を使用して、データ レプリケーションが SSL を介して実行されるように設定します。このウォレットには、迅速な展開を促進する自己署名証明書が含まれています。

  (注) IoT FND RPM にバンドルされている Oracle ウォレットは、自己署名証明書を使用します。カスタム証明書とウォレットを設定して、レプリケーションを円滑に行うことができます。

  (注) SSL を介してデータ レプリケーションを実行しても、パフォーマンスへの影響はありません。

- レプリケーションには、cgms_dev *ではなく*、sys ユーザを使用します。
- パフォーマンスのボトルネックを防止するため、レプリケーションを非同期に設定します。

デフォルトでは、IoT FND は TCP を使用し、ポート 1522 を介してデータベースに接続します。レプリケーションはポート 1622 で TCPS（TCP over SSL）を使用します。

IoT FND データベース HA を設定するためのスクリプトは、IoT FND Oracle Database RPM パッケージ（cgms-oracle-*version_number*.x86_64.rpm）に含まれています。IoT FND データベースをインストールすると、HA スクリプトは $ORACLE_HOME/cgms/scripts/ha に配置されます。

トンネルの冗長性

IoT FND の展開にさらなる冗長性を追加するには、FAR トンネル プロビジョニング グループ内のすべての FAR を複数の ASR に接続する複数のトンネルを設定します。たとえば、すべての FAR に 2 つのトンネルをプロビジョニングするように IoT FND を設定することができます。1 つのトンネルがセルラー インターフェイスを介してアクティブになっている間、冗長トンネルは WiMAX インターフェイスを介して 2 番目の ASR と通信するように設定します。

トンネルの冗長性を設定するには、以下を実行する必要があります。

1. トンネル プロビジョニング グループに ASR を追加します。
2. トンネル プロビジョニング テンプレートを変更して、追加のトンネルを作成するコマンドを含めます。
3. FAR と ASR のインターフェイスで、インターフェイス間のマッピングを決定するポリシーを定義します。
   - トンネル プロビジョニング ポリシーの設定
   - トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

HA の注意事項および制限事項

IoT FND HA の設定に関して、次の点に注意してください。

- IoT FND HA には、FAR、ASR、ロード バランサなどの他のネットワーク コンポーネントの HA サポートは含まれていません。
- IoT FND HA ではゼロ サービス ダウンタイムを目指していますが、これを保証してはいません。
- IoT FND ノードはすべて同じサブネット上にある必要があります。
- IoT FND ノードはすべて、同じようなハードウェアで実行する必要があります。
- すべての IoT FND ノードが同じソフトウェア バージョンを実行する必要があります。
- すべてのノードで IoT FND セットアップ スクリプト（/opt/cgms/bin/setupCgms.sh）を実行します。
- DB の移行のスクリプト（/opt/cgms/bin/db-migrate）は、1 つのノードでのみ実行します。
- /opt/cgms/bin/print_cluster_view.sh スクリプトは、IoT FND クラスタ メンバーに関する情報を表示します。

HA 用の IoT FND インストールの設定

ここでは、IoT FND HA インストールのさまざまな設定について説明します。具体的な内容は次のとおりです。

- HA 用の IoT FND データベースの設定
- IoT FND データベース HA の無効化
- ロード バランシング ポリシー
- LB の実行コンフィギュレーションの例
- トンネル プロビジョニング ポリシーの設定
- トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

HA 用の IoT FND データベースの設定

IoT FND HA データベースを設定するには、次の手順を実行します。

1. スタンバイ データベースを設定します(「スタンバイ データベースの設定」を参照)。

   (注) 必ず最初にスタンバイ データベースを設定します。

   - スタンバイ サーバのデフォルト SID は **cgms_s** で、cgms *ではありません*。
   - HA 用のスタンバイ サーバを設定する前に、スタンバイ サーバの環境変数 $ORACLE_SID が **cgms_s** に設定されていることを確認します。
   - ポートは常に 1522 です。

2. プライマリ データベースを設定します(「プライマリ データベースの設定」を参照)。

   - プライマリ サーバのデフォルト SID は **cgms** です。
   - HA 用のプライマリ サーバを設定する前に、プライマリ サーバの環境変数 $ORACLE_SID が **cgms** に設定されていることを確認します。

3. データベース HA 用に IoT FND を設定します(「データベース HA 用の IoT FND の設定」を参照)。
4. データベース オブザーバを設定します(「オブザーバの設定」を参照)。

スタンバイ データベースの設定

HA 用のスタンバイ データベース サーバを設定するには、setupStandbyDb.sh スクリプトを実行します。このスクリプトでは、プライマリ データベースの IP アドレスなど、スタンバイ データベースに必要な設定情報を入力するように求められます。

```
$ ./setupStandbyDb.sh
$ Are you sure you want to setup a standby database ? (y/n)? y

09-20-2012 13:59:18 PDT: INFO: User response: y
09-20-2012 13:59:18 PDT: INFO: CGMS_S database does not exist.
Enter the SYS DBA password.NOTE: This password should be same as the one set on the primary server:
Re-enter password for SYS DBA:
09-20-2012 13:59:58 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-20-2012 14:00:09 PDT: INFO: User entered CG-NMS DB password.
Enter primary database server IP address: 192.168.1.12
09-20-2012 14:00:27 PDT: INFO: Cleaning up instance - cgms_s
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
…
Total System Global Area  329895936 bytes
Fixed Size    2228024 bytes
Variable Size  255852744 bytes
Database Buffers   67108864 bytes
Redo Buffers    4706304 bytes
...
09-20-2012 14:00:29 PDT: INFO: ========== CGMS_S Database Setup Completed Successfully ==========
```

プライマリ データベースの設定

HA 用のプライマリ データベース サーバを設定するには、setupHaForPrimary.sh スクリプトを実行します。このスクリプトでは、スタンバイ データベースの IP アドレスなど、プライマリ データベースに必要な設定情報を入力するように求められます。

```
$ ./setupHaForPrimary.sh
[oracle@pdb ha]$ ./setupHaForPrimary.sh
09-20-2012 13:58:39 PDT: INFO: ORACLE_BASE: /home/oracle/app/oracle
09-20-2012 13:58:39 PDT: INFO: ORACLE_HOME: /home/oracle/app/oracle/product/11.2.0/dbhome_1
09-20-2012 13:58:39 PDT: INFO: ORACLE_SID : cgms
09-20-2012 13:58:39 PDT: INFO: Make sure the above environment variables are what you expect

Are you sure you wish to configure high availability for this database server ? (y/n)? y

09-20-2012 13:58:45 PDT: INFO: User response: y
Enter standby database server IP address: 192.168.1.10
09-20-2012 13:58:56 PDT: INFO: Secondary listener reachable.Moving on with configuration
mkdir: cannot create directory `/home/oracle/app/oracle/oradata/cgms': File exists
09-20-2012 13:58:58 PDT: INFO: Reloading the listener to pick the new settings

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 13:58:58

…
DGMGRL> 09-20-2012 14:14:54 PDT: INFO: Please start the 'Observer' on appropriate server for ha
monitoring
Total time taken to perform the operation: 975 seconds
09-20-2012 14:14:54 PDT: INFO: ==========  Completed Successfully ==========
```

オブザーバの設定

オブザーバは個別のサーバで実行する必要がありますが、スタンバイ データベースをホストしているサーバで設定できます。

(注) オブザーバの実行に必要なパスワードは、SYS DBA パスワードと同じです。IoT FND Oracle データベースの作成を参照してください。

オブザーバを設定するには、次の手順を実行します。

1. 個別のサーバでオブザーバ スクリプトを実行します。

   ```
   $ ./manageObserver.sh start cgms_s password
   $ DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
   ...
   Welcome to DGMGRL, type "help" for information.
   DGMGRL> Connected.
   DGMGRL> Observer started
   ```

2. getHaStatus.sh スクリプトを実行して、データベースが HA 用に設定されていることを確認します。

   ```
   $ ./getHaStatus.sh
   ...
   Configuration - cgms_dgconfig

     Protection Mode: MaxPerformance
     Databases:
       cgms   - Primary database
       cgms_s - (*) Physical standby database

   Fast-Start Failover: ENABLED

   Configuration Status:
   SUCCESS

   DGMGRL>
   ```

```
Database - cgms

  Role:          PRIMARY
  Intended State:  TRANSPORT-ON
  Instance(s):
    cgms

Database Status:
SUCCESS

DGMGRL>
Database - cgms_s

  Role:          PHYSICAL STANDBY
  Intended State:  APPLY-ON
  Transport Lag:   0 seconds
  Apply Lag:      0 seconds
  Real Time Query: OFF
  Instance(s):
    cgms_s

Database Status:
SUCCESS
```

データベース HA 用の IoT FND の設定

データベース HA 用に IoT FND を設定するには、次の手順を実行します。

1. IoT FND を停止します。
2. setupCgms.sh スクリプトを実行します。

   このスクリプトでは、データベース設定の変更を求められます。**y** を入力します。次に、スクリプトによって、プライマリ データベース サーバの情報（IP アドレス、ポート、データベース SID）を入力するように求められます。この後、スクリプトによって他のデータベース サーバを追加するように求められます。**y** を入力します。次に、スクリプトによって、次のようにスタンバイ データベース サーバの情報（IP アドレス、ポート、データベース SID）を入力するように求められます。

   (注) IoT FND は常にポート 1522 を使用してデータベースと通信します。ポート 1622 は、データベースがレプリケーションのためだけに使用します。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [128.107.154.246]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings.This may take a while.Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password.This may take a while.Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n

09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n

09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

IoT FND データベース HA の無効化

IoT FND データベース HA を無効化するには、次の手順を実行します。

1. オブザーバ プログラムを実行しているサーバで、オブザーバを停止します。

```
$ ./manageObserver.sh stop cgms_s password
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle.All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
$ Observer stopped
```

2. スタンバイ IoT FND データベース サーバで、スタンバイ データベースを削除します。

```
$ ./deleteStandbyDb.sh

Are you sure you want to delete the standby database ? All replicated data will be lost (y/n)? y

09-20-2012 14:27:02 PDT: INFO: User response: y
09-20-2012 14:27:02 PDT: INFO: Cleaning up instance - cgms_s
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle.All rights reserved.
```

```
Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
DGMGRL> DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle.All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Disabled.
DGMGRL> 09-20-2012 14:27:06 PDT: INFO: Removing dataguard configuration
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle.All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Removed configuration
DGMGRL> 09-20-2012 14:27:07 PDT: INFO: Stopping the database

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:27:07 2012

Copyright (c) 1982, 2011, Oracle.All rights reserved.


接続先
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> ORA-01109: database not open


Database dismounted.
ORACLE instance shut down.
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:27:19

Copyright (c) 1991, 2011, Oracle.All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm)(PORT=1522))(CONNECT_DATA=(SERVER=DEDIC
ATED)(SERVICE_NAME=cgms_s)))
The command completed successfully
Cleaning up instance - cgms_s
09-20-2012 14:27:29 PDT: INFO: ==========  Completed Successfully ==========
```

3. プライマリ IoT FND データベース サーバで、HA 設定を削除します。

```
$ ./deletePrimaryDbHa.sh
Are you sure you want to delete the high availability configuration ? All replicated data will be
lost (y/n)? y

09-20-2012 14:25:25 PDT: INFO: User response: y
09-20-2012 14:25:25 PDT: INFO: Removing secondary configuration from primary

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:25:25 2012

Copyright (c) 1982, 2011, Oracle.All rights reserved.


接続先
```

```
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
System altered.
...
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
09-20-2012 14:25:28 PDT: INFO: Removing data guard config files
09-20-2012 14:25:28 PDT: INFO: Removing standby redo logs
09-20-2012 14:25:29 PDT: INFO: Creating listener file
09-20-2012 14:25:29 PDT: INFO: Listener successfully configured.
09-20-2012 14:25:29 PDT: INFO: Recreating tnsnames ora file
09-20-2012 14:25:29 PDT: INFO: reloading the listener

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:29

Copyright (c) 1991, 2011, Oracle.All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
The command completed successfully

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:30

Copyright (c) 1991, 2011, Oracle.All rights reserved.

Starting /home/oracle/app/oracle/product/11.2.0/dbhome_1/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 11.2.0.3.0 - Production
System parameter file is /home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Log messages written to
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
STATUS of the LISTENER
------------------------
Alias                     cgmstns
Version                   TNSLSNR for Linux: Version 11.2.0.3.0 - Production
Start Date                20-SEP-2012 14:25:30
Uptime                    0 days 0 hr.0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
/home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Listener Log File
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))
Services Summary...
Service "cgms" has 1 instance(s).
  Instance "cgms", status UNKNOWN, has 1 handler(s) for this service...
The command completed successfully
09-20-2012 14:25:30 PDT: INFO: ==========  Completed Successfully ==========
```

ロード バランシング ポリシー

次の表に、LB がサポートするトラフィック タイプごとのロード バランシング ポリシーを示します。

Traffic	ロード バランシング ポリシー
ブラウザおよび IoT FND API クライアント（IPv4：ポート 80 および 443）間の HTTPS トラフィック	LB は Web ブラウザおよび IoT FND API クライアントからのすべてのトラフィックにレイヤ 7 の ロード バランシングを使用します。 LB は一般的な HTTPS トラフィックにでスティッキ性を使用します。
ポート 9121 および 9120 に向かう FAR IPv4 トラフィックの場合： ■ HTTPS を介したポート 9120 でのトンネル プロビジョニング ■ HTTPS を介したポート 9121 での通常の定期的な登録	LB はすべての FAR トラフィックにレイヤ 3 のロード バランシングを使用します。これが FAR から IoT FND へのトラフィックです。
メッシュ エンドポイント（ME）との IPv6 CSMP トラフィックの場合： ■ ポート 61624 を介した UDP トラフィック – 登録 – メトリックの定期的な送信 – ファームウェア プッシュ – 設定転送 ■ ポート 61625 を介した UDP トラフィック ME によって送信される停止通知用。	LB はポート 61624 へのすべての ME トラフィックとポート 61625 への停止メッセージに、レイヤ 3 のロード バランシングを使用します。

LB の実行コンフィギュレーションの例

以下に、適切に設定された IoT FND LB の実行コンフィギュレーションの例を示します。

```
# show running-config
Generating configuration....

ssh maxsessions 10

boot system image:c4710ace-t1k9-mz.A5_1_1.bin

hostname cgnmslb2
interface gigabitEthernet 1/1
  switchport access vlan 10
  no shutdown
interface gigabitEthernet 1/2
  description server-side
  switchport access vlan 11
  no shutdown
interface gigabitEthernet 1/3
  description client-side
  switchport access vlan 8
  no shutdown
interface gigabitEthernet 1/4
```

```
  switchport access vlan 55
  no shutdown



access-list ALL line 8 extended permit ip any any
access-list everyone line 8 extended permit ip any any
access-list everyone line 16 extended permit icmp any any
access-list ipv6_acl line 8 extended permit ip anyv6 anyv6
access-list ipv6_acl2 line 8 extended permit icmpv6 anyv6 anyv6



ip domain-lookup
ip domain-name cisco.com
ip name-server 171.68.226.120
ip name-server 171.70.168.183

probe http probe_cgnms-http
  port 80
  interval 15
  passdetect interval 60
  expect status 200 200
  open 1

rserver host 12-12-1-31
  ip address 12.12.1.31
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 12-12-1-32
  ip address 12.12.1.32
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-202
  description realserver 2002:cafe:server::202
  ip address 2002::202
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-211
  ip address 2002:cafe:server::211
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice

serverfarm host cgnms_2
  description cgnms-serverfarm
  probe probe_cgnms-http
  rserver 2002-cafe-server-202 61624
    conn-limit max 4000000 min 4000000
    inservice
  rserver 2002-cafe-server-211 61624
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host cgnms_2_ipv4
  probe probe_cgnms-http
  rserver 12-12-1-31
    conn-limit max 4000000 min 4000000
    inservice
  rserver 12-12-1-32
    conn-limit max 4000000 min 4000000
    inservice
```

```
sticky ip-netmask 255.255.255.255 address source CGNMS_SRC_STICKY
  serverfarm cgnms_2_ipv4


class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any
class-map type management match-all ssh_allow_access
  2 match protocol ssh any
class-map match-any virtual-server-cgnms
  2 match virtual-address 2002:server:cafe::210 udp eq 61624
class-map match-any vs_cgnms_ipv4
  3 match virtual-address 12.12.1.101 tcp eq https
  4 match virtual-address 12.12.1.101 tcp eq 9120
  5 match virtual-address 12.12.1.101 tcp eq 9121
  6 match virtual-address 12.12.1.101 tcp eq 8443
  7 match virtual-address 12.12.1.101 tcp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match virtual_cgnms_l7
  class class-default
    serverfarm cgnms_2
policy-map type loadbalance first-match vs_cgnms_l7_v4
  class class-default
    sticky-serverfarm CGNMS_SRC_STICKY

policy-map multi-match cgnms_policy_ipv6
  class virtual-server-cgnms
    loadbalance vip inservice
    loadbalance policy virtual_cgnms_l7
    loadbalance vip icmp-reply active
policy-map multi-match int1000
  class vs_cgnms_ipv4
    loadbalance vip inservice
    loadbalance policy vs_cgnms_l7_v4
    loadbalance vip icmp-reply active

interface vlan 8
  bridge-group 1
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
interface vlan 10
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  service-policy input int1000
  no shutdown
interface vlan 11
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
interface vlan 55
  bridge-group 1
```

```
  access-group input everyone
  access-group input ipv6_acl
  service-policy input cgnms_policy_ipv6
  no shutdown

interface bvi 1
  ipv6 enable
  ip address 2002:server:cafe::206/64
  no shutdown
interface bvi 2
  ip address 12.12.1.100 255.255.255.0
  no shutdown

domain cisco.com

ip route 2011::/16 2002:server:cafe::101
ip route 2001:server:cafe::/64 2002:cafe::101
ip route 11.1.0.0 255.255.0.0 12.12.1.33
ip route 15.1.0.0 255.255.0.0 12.12.1.33
ip route 13.211.0.0 255.255.0.0 12.12.1.33

context VC_Setup1
  allocate-interface vlan 40
  allocate-interface vlan 50
  allocate-interface vlan 1000

username admin password 5 $1$CB34uAB9$BW8a3ijjxvBGttuGtTcST/  role Admin domain
default-domain
username www password 5 $1$q/YDKDp4$9PkZl1SBMQW7yZ7E.sOZA/  role Admin domain de
fault-domain

ssh key rsa 1024 force
```

トンネル プロビジョニング ポリシーの設定

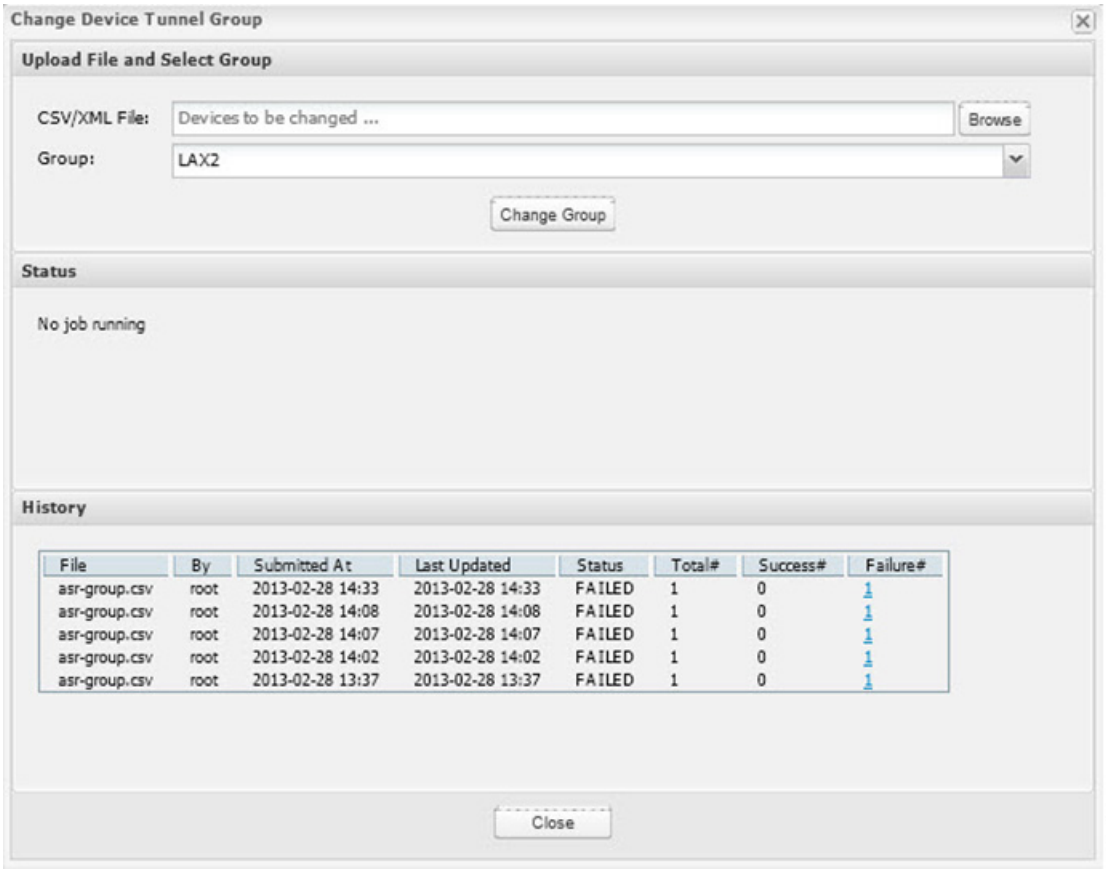
トンネル ポリシーを使用して、FAR に複数のトンネルを設定します。各トンネルは FAR および HER のインターフェイスに関連付けられています。トンネル プロビジョニング グループに 1 つ以上の HER がある場合、IoT FND は [Tunnel Provisioning Policies] タブ（[Config] > [Tunnel Provisioning]）にポリシーを表示します。このポリシーを使用して、FAR と HER 間にインターフェイス マッピングを設定します。

IoT FND で FAR と HER インターフェイスをマッピングするには、次の手順を実行します。

1. [Config] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、トンネルの冗長性を設定するグループを選択します。
3. HER をリストした CSV ファイルまたは XML ファイルを作成して、次のように *EID, device type* の形式でグループに追加します。

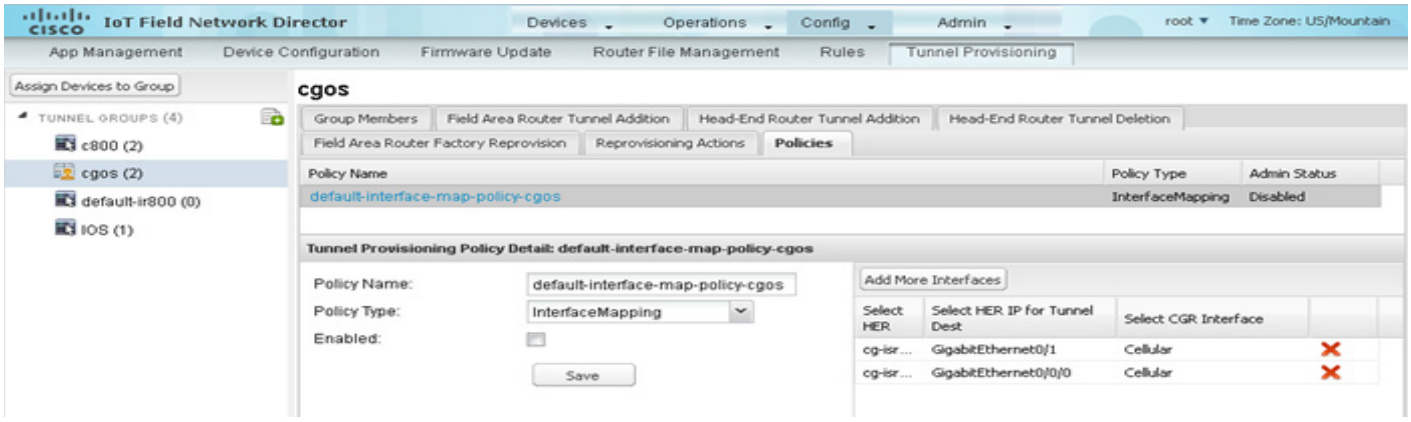
   ```
   eid,deviceType
   asr-0, asr1000
   asr-1, asr1000
   asr-2, asr1000
   ```

4. [Assign Devices to Group] をクリックして、ファイルをインポートして HER をグループに追加します。



(注)HER は複数のトンネル プロビジョニング グループのメンバーになることができます。

5. トンネル プロビジョニング グループを選択し、[Policies] タブをクリックします。

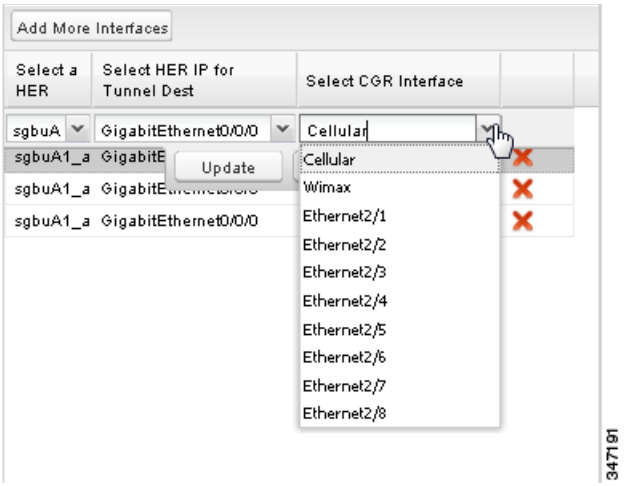


デフォルトでは、IoT FND は InterfaceMapping ポリシーを表示します。

(注)InterfaceMapping は、現在 IoT FND でサポートされている唯一のポリシー タイプです。

IoT FND はグループ内のすべての HER に対して 1 つのインターフェイス マッピング エントリを表示します。インターフェイス マッピング エントリは、必要に応じて追加または削除することができます。

6. [Policy Name] フィールドに、ポリシーの名前を入力します。
7. ポリシーにインターフェイス マッピング エントリを追加するには、[Add More Interfaces] をクリックします。



エントリを削除するには、そのエントリの [Delete]( )をクリックします。

8. インターフェイス マッピング エントリを設定するには、ポリシー名のリンクをクリックし、必要に応じて以下を実行します。
   a. 別の HER を選択するには、現在選択されている HER をクリックして、[Select a HER] ドロップダウン メニューから別の HER を選択します。
   b. HER でトンネル先の HER IP を選択するには、選択されているインターフェイスをクリックして、[Select HER IP] ドロップダウン メニューから別の HER IP を選択します。
   c. 選択した HER インターフェイスにマップする FAR インターフェイスを選択するには、[Select CGR Interface] ドロップダウン メニューからインターフェイスを選択します。
   d. [Update] をクリックします。
9. ポリシーを有効にするには、[Enabled] チェック ボックスをオンにします。
10. [Save(保存)] をクリックします。

トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

トンネル プロビジョニング グループにトンネル プロビジョニング ポリシーを設定したら、フィールド エリア ルータ トンネル追加テンプレートとヘッドエンド ルータ トンネル追加テンプレートを変更して、ポリシーで定義された複数のトンネルを確立するためのコマンドを含めます。

フィールド エリア ルータ トンネル追加テンプレートの例

この例では、太字は、複数のトンネルを作成するために行ったデフォルトのフィールド エリア ルータ トンネル追加テンプレートへの変更を示しています。

```
<#--
  Configure a Loopback0 interface for the FAR.This is done first as features
  look for this interface and use it as a source.

  This is independent of policies
-->
interface Loopback0
  <#--
```

```
    Now obtain an IPv4 address that can be used to for this FAR's Loopback
    interface.The template API provides methods for requesting a lease from
    a DHCP server.The IPv4 address method requires a DHCP client ID and a link
    address to send in the DHCP request.The 3rd parameter is optional and
    defaults to "CG-NMS".This value is sent in the DHCP user class option.
    The API also provides the method "dhcpClientId".This method takes a DHCPv6
    Identity association identifier (IAID) and a DHCP Unique  IDentifier (DUID)
    and generates a DHCPv4 client identifier as specified in RFC 4361.This
    provides some consistency in how network elements are identified by the
    DHCP server.
  -->
  ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32
  <#--
    Now obtain an IPv6 address that can be used to for this FAR's loopback
    interface.The method is similar to the one used for IPv4, except clients
    in DHCPv6 are directly identified by their DUID and IAID.IAIDs used for
    IPv4 are separate from IAIDs used for IPv6, so we can use zero for both
    requests.
  -->
  ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128
exit

<#-- Make certain the required features are enabled on the FAR.-->
feature crypto ike
feature ospf
feature ospfv3
feature tunnel
<#-- Features ike and tunnel must be enabled before ipsec.-->
feature crypto ipsec virtual-tunnel

<#--
  Toggle on/off the c1222r feature to be certain it uses the Loopback0
  interface as its source IP.
-->
no feature c1222r
feature c1222r

<#-- Configure Open Shortest Path First routing processes for IPv4 and IPv6.-->
router ospf 1
exit
router ospfv3 2
exit

<#--
  Now that OSPF has been configured complete the configuration of Loopback0.
-->
interface Loopback0
  ip router ospf 1 area ${far.ospfArea1!"1"}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
exit

<#-- Configure Internet Key Exchange for use by the IPsec tunnel(s).-->
crypto ike domain ipsec
  identity hostname
  policy 1
    <#-- Use RSA signatures for the authentication method.-->
    authentication rsa-sig
    <#-- Use the 1536-bit modular exponential group.-->
    group 5
  exit
exit
crypto ipsec transform-set IPSecTransformSet esp-aes 128 esp-sha1-hmac
crypto ipsec profile IPSecProfile
```

```
  set transform-set IPSecTransformSet
exit

<#--
  Define template variables to keep track of the next available IAID (IPv4)
  and the next available tunnel interface number.We used zero when leasing
  addresses for Loopback0, so start the IAID at one.
-->
<#assign iaId = 1>
<#assign interfaceNumber = 0>

<#--
  The same logic is needed for each of the IPsec tunnels, so a macro is used
  to avoid duplicating configuration.The first parameter is the prefix to
  use when looking for the WAN interface on the FAR to use for the source of
  the tunnel.The second parameter is the OSPF cost to assign to the tunnel.
-->
<#macro configureTunnel interfaceNamePrefix destinationInterface her tunnelIndex ospfCost>
  <#--
    If an interface exists on the FAR whose name starts with the given prefix
    and an IPv4 address as been assigned to that interface then the IPsec
    tunnel can be configured, otherwise no tunnel will be configured.The
    template API interfaces method will return all interfaces whose name
    starts with the given prefix.
  -->
  <#assign wanInterface = far.interfaces(interfaceNamePrefix)>
  <#-- Check if an interface was found and it has an IPv4 address.-->
  <#if (wanInterface[0].v4.addresses[0].address)??>
    <#--
      Determine the HER destination address to use when configuring the tunnel.
      If the optional property "ipsecTunnelDestAddr1" has been set on this FAR
      then use the value of that property.Otherwise look for that same property
      on the HER.If the property is not set on the FAR or the HER, then fallback
      to using an address on the HER GigabitEthernet0/0/0 interface.
    -->
    <#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

    <#if !(destinationAddress??)>
      ${provisioningFailed("Unable to determine the destination address for IPsec tunnels")}
    </#if>
    interface Tunnel${interfaceNumber}
      <#assign interfaceNumber = interfaceNumber + 1>
      description IPsec tunnel to ${her.eid}
      <#--
        For a tunnel interface two addresses in their own tiny subnet are
        needed.The template API provides an ipv4Subnet method for leasing an
        IPv4 from a DHCP server.The parameters match those of ipv4Address,
        with a fourth optional parameter that can be used to specify the
        prefix length of the subnet to request.If not specified the prefix
        length requested will default to 31, which provides the two addresses
        needed for a point to point link.

        NOTE: If the DHCP server being used does not support leasing an IPv4
        subnet, then this call will have to be changed to use the ipv4Address
        method and the DHCP server will have to be configured to respond
        appropriately to the request made here and the second request that
        will have to be made when configuring the HER side of the tunnel.
        That may require configuring the DHCP server with reserved addresses
        for the client identifiers used in the calls.
      -->
      <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
      <#assign iaId = iaId + 1>
      <#-- Use the second address in the subnet for this side of the tunnel.-->
      ip address ${lease.secondAddress}/${lease.prefixLength}
      ip ospf cost ${ospfCost}
```

```
      ip ospf mtu-ignore
      ip router ospf 1 area ${far.ospfArea1!"1"}
      tunnel destination ${destinationAddress}
      tunnel mode ipsec ipv4
      tunnel protection ipsec profile IPSecProfile
      tunnel source ${wanInterface[0].name}
      no shutdown
    exit
  </#if>
</#macro>

<#--
  Since we are doing policies for each tunnel here, the list of policies passed to this template can be
  iterated over to get the tunnel configuration viz interface mapping

  tunnelObject.ipSecTunnelDestInterface is the "interface on CGR"
  tunnelObject.ipSecTunnelSrcInterface is the "interface on HER"
  tunnelObject.her is the HER of interest
 -->

<#list far.tunnels("ipSec") as tunnelObject>
    <@configureTunnel tunnelObject.ipSecTunnelDestInterface tunnelObject.ipSecTunnelSrcInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>  <----- Loop through policies (aka Tunnels)
</#list>

<#--
  Make certain provisioning fails if we were unable to configure any IPsec
  tunnels.For example this could happen if the interface properties are
  set incorrectly.
-->
<#if iaId = 1>
  ${provisioningFailed("Did not find any WAN interfaces to use as the source for IPsec tunnels")}
</#if>

<#--
  Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
  center.
-->
<#macro configureGreTunnel destinationInterface her tunnelIndex>

<#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

<#if !(destinationAddress??)>
     ${provisioningFailed("Unable to determine the destination address for GRE tunnels")}
</#if>

interface Tunnel${interfaceNumber}
  <#assign interfaceNumber = interfaceNumber + 1>
  description GRE IPv6 tunnel to ${her.eid}
  <#--
    The ipv6Subnet method is similar to the ipv4Subnet method except instead
    of obtaining an IPv4 subnet it uses DHCPv6 prefix delegation to obtain an
    IPv6 prefix.The prefix length will default to 127, providing the two
    addresses needed for the point to point link.For the IAID, zero was used
    when requesting an IPv6 address for loopback0, so use one in this request.
  -->
  <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
  ipv6 address ${lease.secondAddress}/${lease.prefixLength}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
  ospfv3 mtu-ignore
  tunnel destination ${destinationAddress}
  tunnel mode gre ip
  tunnel source Loopback0
```

```
  no shutdown
exit

</#macro>

<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
    <@configureGreTunnel greTunnelObj.greDestInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```

ヘッドエンド ルータ トンネル追加テンプレート

この例では、太字は、複数のトンネルを作成するために行ったデフォルトのヘッドエンド ルータ トンネル追加テンプレートへの変更を示しています。

```
<#--
  Define template variables to keep track of the IAID (IPv4) that was used by
  the FAR template when configuring the other end of the tunnel.This template
  must use the same IAID in order to locate the same subnet that was leased by
  the FAR template so both endpoints are in the matching subnet.
-->
<#assign iaId = 1>

<#--
  The same logic is needed for each of the IPsec tunnels, so a macro is used.
-->
<#macro configureTunnel ipSecTunnelSrcInterface ipSecTunnelDestInterface her tunnelIndex ospfCost>
  <#--
    Only configure the HER tunnel end point if the FAR tunnel end point was
    configured.This must match the corresponding logic in the FAR tunnel
    template.The tunnel will not have been configured if the WAN interface
    does not exist on the FAR or does not have an address assigned to it.
  -->
  <#assign wanInterface = far.interfaces(ipSecTunnelDestInterface)>
  <#if (wanInterface[0].v4.addresses[0].address)??>
    <#-- Obtain the full interface name based on the prefix.-->
    <#assign interfaceName = wanInterface[0].name>
    <#--
      Locate a tunnel interface on the HER that is not in use.The template
      API provides an unusedInterfaceNumber method for this purpose.All of
      the parameters are optional.The first parameter is a name prefix
      identifying the type of interfaces, it defaults to "tunnel".The second
      parameter is a lower bound on the range the unused interface number must
      be in, it defaults to zero.The third parameter is the upper bound on
      the range, it defaults to max integer (signed).The method remembers
      the unused interface numbers it has returned while the template is
      being processed and excludes previously returned numbers.If no unused
      interface number meets the constraints an exception will be thrown.
    -->
    interface Tunnel${her.unusedInterfaceNumber()}
      description IPsec tunnel to ${far.eid}
      <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
      <#assign iaId = iaId + 1>
      ip address ${lease.firstAddress} ${lease.subnetMask}
      ip ospf cost ${ospfCost}
      ip ospf mtu-ignore
      tunnel destination ${wanInterface[0].v4.addresses[0].address}
      tunnel mode ipsec ipv4
      tunnel protection ipsec profile IPSecProfile
      tunnel source ${ipSecTunnelSrcInterface}
      no shutdown
    exit
    router ospf 1
```

```
      network ${lease.prefix} ${lease.wildcardMask} area ${far.ospfArea1!"1"}
    exit
  </#if>
</#macro>

<#list far.tunnels("ipSec") as tunnelObject>
        <@configureTunnel tunnelObject.ipSecTunnelSrcInterface tunnelObject.ipSecTunnelDestInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>
</#list>

<#--
  Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
  center.
-->
<#macro configureGreTunnel greSrcInterface her tunnelIndex>
interface Tunnel${her.unusedInterfaceNumber()}
  description GRE IPv6 tunnel to ${far.eid}
  <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
  ipv6 address ${lease.firstAddress}/${lease.prefixLength}
  ipv6 enable
  ipv6 ospf 2 area ${far.ospfV3Area1!"0"}
  ipv6 ospf mtu-ignore
  tunnel destination ${far.interfaces("Loopback0")[0].v4.addresses[0].address}
  tunnel mode gre ip
  tunnel source ${greSrcInterface}
exit
</#macro>

<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
        <@configureGreTunnel greTunnelObj.greSrcInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```

IoT FNDのトラブルシューティング

ここでは、IoT FND の一般的な問題の解決方法について説明します。

(注)IoT FND のバージョンについて、常にリリース ノートを参照するようにしてください。

トンネル プロビジョニングの DHCP 設定問題

アドレスの割り当てに問題があると、IoT FND は Tunnel Provisioning Failure イベントをログに記録します。ログ エントリにエラーの詳細が記述されます。

アドレスの割り当てプロセスをモニタするには、次の手順を実行します。

- IoT FND の server.log ファイルをチェックし、IoT FND がトンネルのプロビジョニング時に DHCP 要求を送信しているかを確認します。
- DHCP サーバのログ ファイルをチェックし、IoT FND からの DHCP 要求が DHCP サーバに到達したかを確認します。

要求がサーバに到達していない場合は、次の手順を実行します。

- IoT FND の [Provisioning Settings] ページ([Admin] > [System Management] > [Provisioning Settings])で、DHCP サーバのアドレスが正しいことを確認します。
- IoT FND と DHCP サーバとの間のネットワーク問題を確認します。

DHCP サーバが要求を受信しているにもかかわらず応答していない場合は、次の手順を実行します。

- DHCP サーバのログ ファイルを確認し、DHCP サーバが DHCP 要求に含まれるリンク アドレスからの要求をサポートするよう設定されていることを確認します。リンク アドレスはトンネル プロビジョニング　テンプレートで定義されています。
- DHCP サーバのアドレス プールが満杯でないことを確認します。

DHCP サーバが応答をしていても IoT FND が応答を処理していない場合は、次の手順を実行します。

- リース時間の無限であることを確認します。そうでない場合、IoT FND は応答を処理しません。
- 他のエラーについて、DHCP サーバのログと IoT FND サーバのログを確認します。

メッシュ エンドポイントの登録の問題

ME が IoT FND に登録した理由を確認するために、IoT FND は ME から登録理由コードを収集し、登録問題を診断するのに役立つよう、イベントおよび印刷されたキー値ペアなどの他の関連情報を含むコードをロギングします。

次に、ロギングされたイベントの例を示します。

```
?Event logged: Event(id=0, eventTime=1335304407477, eventSeverity=0, eventSource=cgmesh,
eventMessage=Mesh node registered due to cold  boot: [lastReg: 0, lastRegReason: 1],
NetElement.id=10043, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null
```

表 1 に、ME 登録の理由コードと関連イベントをリスト表示します。

表 1　　メッシュ エンドポイント登録の理由コード

登録の理由コード	コード	イベント タイプの名前	重大度	メッセージ	説明
REASON_UNKNOWN	0	unknownRegReason	INFO	Mesh node registered for unknown reason.	
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	メッセージには、ME の新しい IP アドレスが含まれます。
REASON_ADMIN	2	manualReRegistration	INFO	Mesh node registered due to manual registration.	エンドポイントは、URL フィールドを含まない NMSRedirectRequest を受信しました。
REASON_IP_CHANGE	3	rejoinedWithNewIP	INFO	Mesh node registered with new IP address.	メッセージには、ME の新しい IP アドレが含まれます。
REASON_NMS_CHANGE	4	nmsAddrChange	INFO	Mesh node registered due to NMS address change.	IoT FND の IP アドレスは、NMSRedirect の外部で変更されました（新しい DHCPv6 オプション値が受信されました）。
REASON_NMS_REDIRECT	5	manualNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	エンドポイントは NMSRedirect 要求を受信しました。
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	エンドポイントは、IoT FND からエラーを受信しました。

ME の IoT FND への登録時にイベントを生成する以外に、IoT FND は、WPAN 変更の TLV `WPANStatus` を受信した後にもイベントを生成します。

```
Event logged: Event(id=0, eventTime=1335304407974, eventSeverity=0, eventSource=cgmesh,
eventMessage=WPAN change due to migration to better PAN: [lastChanged: 0, astChangedReason: 4],
NetElement.id=10044, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

表 2 に、ME の WPAN 変更の理由と対応するイベントを示します。

表 2　メッシュ エンドポイントの WPAN 変更の理由

登録の理由コード	コード	Event Name	重大度タイプ	説明
IEEE154_PAN_LEAVE_UNKNOWN	-1	unknownWPANChange	MAJOR	不明な理由による WPAN 変更。
IEEE154_PAN_LEAVE_INIT	0	meshInit	該当なし	このコードのイベントは生成されません。
IEEE154_PAN_LEAVE_SYNC_TIMEOUT	1	meshConnectivityLost	MAJOR	メッシュ接続の切断による WPAN 変更。
IEEE154_PAN_LEAVE_GTK_TIMEOUT	2	meshLinkKeyTimeout	MAJOR	メッシュ リンク キーのタイムアウトによる WPAN 変更。
IEEE154_PAN_LEAVE_NO_DEF_ROUTE	3	defaultRouteLost	MAJOR	デフォルト ルートの不在による WPAN 変更。
IEEE154_PAN_LEAVE_OPTIMIZE	4	migratedToBetterPAN	MAJOR	より良好な PAN への移行による WPAN 変更。

これらのイベントでは、ME がネットワークから切断されてから再接続するまでの経過時間がメッセージに含められます。IoT FND は、イベントがロギングされてから ME がオフラインだった期間の合計を示します（たとえば 4 hours 23 minutes ago）。

期限切れデータベース パスワードの回復

期限切れパスワードを回復するには、次のコマンドを実行します。

```
su - oracle

sqlplus sys/cgmsDbaAccount@cgms as sysdba
  alter user cgms_dev identified by test;
  alter user cgms_dev identified by password;
  exit;
```

IoT FND データベース パスワードのロック解除

不正な IoT FND データベース パスワードを何回も入力すると、Oracle はユーザ アカウントをロックします。Oracle ソフトウェアを次の例のように使用して、パスワードをロック解除してください。

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
  alter user cgms_dev account unlock;
  exit;
```

IoT FND サービスが開始しない

IoT FND サービスが開始しない場合は、次の手順を実行します。

1. データベースへの接続を確認します。
   a. IoT FND サーバにルートとしてログインします。
   b. コマンド プロンプトで次のコマンドを入力します。

```
service cgms status
```

c. データベース サーバの IP アドレスと、IoT FND がデータベースに接続できることを確認します。

- IP アドレスが正しくないかまたは IoT FND がデータベースにアクセスできない場合は、**setupCgms.sh** を実行して正しい値を入力します。

d. **service cgms status** コマンドを実行して接続を確認します。

e. IoT FNDを起動します。

2. サーバにインストールされている JRE のバージョンが正しいことを確認します(「システム要件」を参照)。
3. データベースの移行が正常に実行されたことを確認します。

IoT FND サーバの server.log ファイルに例外がある

server.log ファイルに IoT FND が cgms_keystore ファイルを開けなかったことを示す例外が存在する場合は、IoT FND サーバの cgms.properties ファイルに保存されている cgms_keystore パスワードが正しくありません。

cgms_keystore ファイルのパスワードは、暗号化されて /opt/cgms/server/cgms/conf/cgms.properties ファイルに保存されます。

パスワードを暗号化または復号化するには、/opt/cgms/bin/**encryption_util.sh** スクリプトを使用します。

cgms.properties ファイルでパスワードを確認または更新します。更新が必要な場合は、パスワードを変更した後に IoT FND を再起動します。

ルート パスワードのリセット

IoT FND のルート ユーザ アカウントのパスワードを忘れた場合は、/opt/cgms/bin/**password_admin.sh** スクリプトを実行してパスワードをリセットします。

IoT FND のセカンド サーバがクラスタを形成しない

通常、IoT FND クラスタでのノードの検出は自動的に行われます。複数の IoT FND サーバが同じサブネットに存在すると、クラスタが形成されます。

IoT FND サーバをインストールしたときに、そのサーバがクラスタに参加しない場合は、以下を行ってください。

1. サーバが同じサブネットにあること、相互に ping できること、および同じクラスタ名を共有していることを確認します。
2. /opt/cgms/bin/print_cluster_view.sh スクリプトを実行して、すべてのメンバーのステータスを確認します。
3. クラスタの名前を次のように変更します。
   a. IoT FND のすべてのクラスタ ノードで、HA_PARTITION_NAME パラメータの値を変更してから再起動します。
   b. UDP_MULTICAST_ADDR パラメータの値(一意のマルチキャスト アドレス)を、クラスタ内のすべてのノードに一致するよう変更します。
   c. CLUSTER_BIND_ADDR パラメータの値を、NMS のバインド先とするインターフェイスに変更します。
4. すべてのクラスタ ノードが NTP を使用するよう設定されていることを確認します(「NTP サービスの設定」を参照)。
5. /etc/hosts ファイルを確認し、IP アドレスがローカル サーバのホスト名に正しくマップされていることを確認します。

サービスが自動的に再起動するIoT FND

IoT FND サービスを開始すると、ウォッチドッグ スクリプトが呼び出されます。ウォッチドッグ スクリプトは、IoT FND サービスの状態を確認します。異常を検出すると、ウォッチドッグ スクリプトはその状態を /opt/cgms/server/cgms/log/cgms_watchdog.log ファイルに記録します

ウォッチドッグ スクリプトは、異常な状態が改善したかどうかを判断するために、3 回試行されます。改善しない場合、データベースが到達不能になっていなければ、IoT FND サービスは自動的に再起動します。データベースが到達可能でない場合、ウォッチドッグは IoT FND サービスを停止します。再起動した原因を確認するには、server.log などのログ ファイルを確認します。

IoT FND サーバでルートとして /opt/cgms/bin/deinstall_cgms_watchdog.sh スクリプトを実行することにより、手動でウォッチドッグ プロセスを無効にします。

FAR の管理に関する問題

ここでは、FAR の管理に関する一般的な問題と解決方法について説明します。

証明書の例外

FAR の IoT FND への登録試行時に IoT FND サーバに保存された server.log ファイルに次の例外が表示された場合は、cgms_keystore ファイルに CA サーバ証明書が含まれていないか、または cgms_keystore ファイルにインポートされている CA 証明書が正しくありません。

```
SSLException: Received fatal alert: unknown_ca
```

cgms_keystore ファイルに証明書をインポートする方法については、「証明書の生成およびインストール」を参照してください。

FAR がリロードし続け、Up の状態に切り替わらない

FAR が IoT FND に接続するたびにリロードし続ける場合、IoT FND が FAR にプッシュした設定が正常に適用されていないためである可能性があります。

設定のプッシュが失敗した原因を確認するには、IoT FND サーバの server.log ファイルをチェックします。[Field Area Router Tunnel Addition] テンプレートへの入力ミスが失敗の原因である場合もあります（IoT FND は、テンプレートを検証しません）。

(注) FAR が IoT FND に登録すると、IoT FND は、show コマンドにより FAR に対してクエリを実行します。IoT FND はその後、[Field Area Router Tunnel Addition] テンプレート内の設定コマンドに基づいて FAR を設定します。

リロードが続く原因には、他に次のものが考えられます。

- パケットをドロップして登録を完了させないようにする、不正な WAN リンク。
- ファイアウォール の問題。ファイアウォールが両方向のトラフィックを許可していること、および、正しいポートを入出力するトラフィックの通過が許可されていることを確認します。

IoT FND で FAR の状態が正しくない

IoT FND で、FAR の ping や FAR へのルートのトレースを問題なく実行できるにもかかわらず、FAR の状態が [Down] と表示される場合があります。

IoT FND は、FAR 上で実行される IoT DM サービスを介して FAR を管理します。そのため、FAR を ping でき、FAR が到達可能な場合も、次により、jetty サーバおよび Call Home 機能が FAR で有効であることを確認する必要があります。

```
'show run callhome' should have 'enable' in the config and 'sh jvm status'
```

メッシュ エンドポイントの管理の問題

ここでは、ME の管理に関する一般的な問題と解決方法について説明します。

メッシュ エンドポイントが IoT FND に登録していない

ME が FAR に接続していること、および IPv6 により IoT FND から ping できることを確認します。ping できる場合は、以下を確認してください。

- クロックが同期されている。
- ME により使用されている DHCP サーバが正しい IoT FND IP アドレスでプログラムされている。
- ME が実行しているイメージが、現在のバージョンの IoT FND と互換性がある。
- HSM が使用されている場合、HSM がオンラインで適切に応答していることが必要です。

ライセンスの問題

ここでは、ライセンスの管理に関する一般的な問題と解決方法について説明します。

デバイス インポートの失敗

IoT FND へのデバイス インポートは、IoT FND サーバ ライセンスの割り当て数に依存します。

IoT FND サーバのライセンス数が、IoT FND データベースにインポートするデバイスの数およびタイプに十分に対応できることを確認します。

IoT FND では、一意のデバイス EID のみが許可されます。IoT FND にこのデバイス EID を インポート済みであったり、現在同じデバイス EID をインポートしようとしているユーザが他にいないことを確認します。他のユーザが同時に同じデバイスを IoT FND にインポートしていないことを確認します。

ライセンス ファイルのアップロードの失敗

期限切れのライセンス ファイルはエラーの原因になります。ライセンス ファイルの有効性および有効期限を確認してください。