



デバイスの管理

この章の内容は、次のとおりです。

- [概要 \(6-1 ページ\)](#)
- [デバイスのカスタム設定 \(6-1 ページ\)](#)
- [ハブ デバイスの交換 \(6-5 ページ\)](#)

概要

各ハブ サイトやブランチ サイトには 1 つ以上のデバイスを関連付けることができます。IWAN アプリは、ネットワーク内のデバイスに対するバッチ CLI コマンドの実行を有効化するカスタム設定機能など、デバイスを個別に管理する手段を提供します。

デバイスのカスタム設定

カスタム設定は、IWAN ネットワーク内のデバイスに対して CLI 設定コマンドを実行するためのメカニズムです。この機能はコマンドをバッチ ファイルで実行する場合と同じように機能しますが、IWAN アプリからリモートで動作します。一連のコマンドを入力し(後で使用するために任意に保存)、設定コマンドを実行するデバイスを選択します。IWAN アプリは指定されたデバイスにコマンドを送信し、コマンドの実行が成功したか否かを示します。

コマンドが失敗した場合のロールバック メカニズム

コマンドの実行に失敗した場合、この機能はロールバック メカニズムを備えているので、失敗した設定操作を無効にする一連のコマンドを実行できます。

デバイスごとに設定できるパラメータ

カスタム設定には、コマンドが実行されている各デバイスに固有のパラメータ値を入力するように実行時に求める「パラメータ」機能があります。設定を実行すると、選択したターゲット デバイスごとに値を 1 つずつ入力することを求められます。パラメータは、ドル記号 (\$) の後にパラメータ名が続く形式で表示されます。

例: \$interface

最大 10 個のパラメータを使用できます。

カスタム設定のデフォルト テンプレート

IWAN アプリには、さまざまなネットワーキング機能に CLI レベルのサポートを提供するデフォルト設定テンプレートが含まれています。各テンプレートは、事前定義済み機能を実行するための一連の CLI コマンドで構成されます。テンプレートには「デバイスごとに設定できるパラメータ」が含まれていることがあります。その場合、設定を実行すると、選択したターゲット デバイスごとに値を1つずつ入力することを求められます。

次の表は、デフォルトで含まれている設定テンプレートの概要を示します。

表 6-1 カスタム設定のデフォルト テンプレート

テンプレート	説明
Liveaction フロー	<p>LiveAction ネットワーク監視を有効にします。</p> <p>LiveAction と互換性がある NetFlow モニタを設定し、LiveAction サーバをエクスポートするようにモニタを設定します。</p> <p>次のいずれかのテンプレートを選択します。</p> <ul style="list-style-type: none"> • LiveAction-SR1L: 1 つの WAN リンクを備えたシングル ルータ • LiveAction SR2L: 2 つの WAN リンクを備えたシングル ルータ • LiveAction SR3L: 3 つの WAN リンクを備えたシングル ルータ <p>テンプレートを実行する際に、次のものを入力する必要があります。</p> <ul style="list-style-type: none"> • LIVEACTION_IP- IP: LiveAction サーバのアドレス。 例: 10.1.0.10 • TUN_INTERFACE: DMVPN トンネル インターフェイスの名前。 例: Tunnel10
ダイレクトインターネットアクセス	<p>ダイレクト インターネット アクセス (DIA) を設定します。</p> <p>NAT、ゾーン ベースのポリシー ファイアウォール (ZFW)、およびポリシー ベース ルーティング (PBR) をブランチからのダイレクト インターネット アクセス用に設定します。また、テンプレートは、インターネット ゲートウェイ IP のトラッキング、およびインターネット ゲートウェイが到達不能の場合にはトンネル オーバーレイへのフェールオーバーを設定します。</p> <p>(注) DIA 設定テンプレートは、Cisco ISR 4000 シリーズ ルータにのみ適用されます。</p> <p>テンプレートを実行する際に、次のものを入力する必要があります。</p> <ul style="list-style-type: none"> • LAN_SUBNET: LAN のサブネット アドレス (ワイルドカード マスクを使用)。 例: 10.1.0.0 0.0.255.255 • INET_WAN_INTERFACE_NAME: インターネット WAN インターフェイスの名前。 例: GigabitEthernet 0/0/0 • INET_VRF_NAME: WAN インターフェイス上で適用された FVRF の名前。 例: IWAN-TRANSPORT-2 • INET_GW_IP: インターネット ゲートウェイの IP アドレス。 例: 70.70.70.2 • LAN_INTERFACE_NAME: LAN インターフェイスの名前。 例: GigabitEthernet0/0/2

表 6-1 カスタム設定のデフォルト テンプレート (続き)

テンプレート	説明
ゲスト インターネット アクセス	<p>ゲスト インターネット アクセスを IWAN ブランチ ルータで有効にします。</p> <p>ルータ上のゲスト VLAN インターフェイスを NAT およびゾーン ベースのポリシー ファイアウォール (ZFW) とともに作成します。ゲスト VLAN は、IWAN-GUEST と呼ばれる別個の VRF に割り当てられます。</p> <p>テンプレートを実行する際に、次のものを入力する必要があります。</p> <ul style="list-style-type: none"> • INET_WAN_INTERFACE_NAME: インターネット WAN インターフェイスの名前。 例: GigabitEthernet 0/0/0 • INET_GW_IP: インターネット ゲートウェイの IP アドレス。 例: 70.70.70.2 • GUEST_SUBNET: ゲスト VLAN のサブネット アドレス (ワイルドカード マスクを使用)。 例: 10.2.10.0 0.0.0.255 • GUEST_INTERFACE_NAME: ゲスト VLAN に使用されるサブインターフェイスの名前。 例: GigabitEthernet 0/0/0.66 • GUEST_VLAN_ID: ゲスト VLAN の VLAN ID 番号。 例: 66 • GUEST_INTERFACE_IP: ゲスト VLAN インターフェイスの IP アドレス (マスクを使用)。 例: 10.1.10.1 255.255.255.0 • GUEST_MASK: ゲスト VLAN インターフェイスに使用されるサブネット マスク。 例: 255.255.255.0

カスタム設定の有効化

カスタム設定機能による CLI 設定コマンドの実行を有効にするには、次の手順を実行します。

手順

- 手順 1** サイト リスト ページで、テーブルの上部にある歯車アイコンをクリックして [Custom Config Status] を選択し、[Custom Config Status] 列を表示します。列が表示され、テーブルの上部に [Custom Config] ボタンが表示されます。

カスタム設定の作成と実行

[Custom Configuration] ウィンドウを開いて、カスタム設定の CLI バッチ ファイルを作成したり、既存のカスタム設定 (テンプレート) を実行したりするには、次の手順を実行します。

手順

- 手順 1** サイト リスト ページで、テーブルの上部にある [Custom Config] ボタンをクリックします。ボタンが表示されない場合は、[カスタム設定の有効化 \(6-3 ページ\)](#) を参照してください。[Custom Config] ページが表示されます。

- 手順 2 既存のカスタム設定を選択するか、プラス記号アイコン(+)をクリックして新しいカスタム設定を作成します。
- 手順 3 [Actual] ペインで、バッチ CLI コマンド ファイルの場合と同様に、実行する CLI コマンドを入力します。コマンドは、デバイスに対してコンフィギュレーション モードで実行されます。



(注) IWAN アプリは入力されたコマンドを検証しません。

- 手順 4 (任意) 選択したすべてのデバイスに対してコマンドのフルセットを実行します。設定コマンドを実行する各デバイス固有のパラメータを個々に入力するには、CLI コマンドで「パラメータ」値を使用します(パラメータ名の前にドル記号(\$)を付けます)。
例: \$interface
カスタム設定を実行すると、選択したターゲット デバイスごとにこの「パラメータ」の値を 1 つずつ入力することを要求されます。最大 10 個のパラメータを使用できます。
- 手順 5 [Rollback] ペインで、[Actual] ペインの設定コマンドの 1 つ以上が正常に実行されなかった場合に実行するコマンドを入力します。カスタム設定コマンドの実行に失敗した場合の対処方法については、[カスタム設定の実行に失敗した場合の対処方法\(6-4 ページ\)](#)を参照してください。
- 手順 6 [Devices] ペインで、CLI 設定コマンドを実行するデバイスを選択します。
- 手順 7 [Save] をクリックして、設定を実行せずに保存します。[Deploy] をクリックして、指定したデバイスに対して設定を実行します。サイト リスト ページが自動的に開き、設定コマンドの実行ステータス([Success] または [Failure])を表示できるようになります。

カスタム設定の実行ステータスの表示

サイト リスト ページの [Custom Config Status] 列には、設定コマンドの実行ステータス([Success] または [Failure])がサイトごとに表示されます。

サイト内のいずれかのデバイスで実行に失敗した場合は、そのサイトの [Custom Config Status] 列に [Failure] と表示されます。エラーが発生した場合は、[Custom Config Status] 列の [Failure] リンクをクリックすると、サイト内の各デバイスのステータスが表示されます。カスタム設定の実行に失敗した場合の対処方法については、[カスタム設定の実行に失敗した場合の対処方法\(6-4 ページ\)](#)を参照してください。

カスタム設定の実行に失敗した場合の対処方法

CLI カスタム設定コマンドの実行に失敗した場合は、次の手順を実行して対処します。

手順

- 手順 1 サイト リスト ページの [Custom Config Status] 列には、設定コマンドの実行ステータス([Success] または [Failure])がサイトごとに表示されます。サイト内のいずれかのデバイスで実行に失敗した場合は、そのサイトの [Custom Config Status] 列に [Failure] と表示されます。エラーが発生した場合は、[Custom Config Status] 列の [Failure] リンクをクリックすると、[Site Details] ポップアップが開きます。

手順 2 [Site Details] ポップアップには、サイト内の各デバイスのステータスが表示されます。スタートスが [Failure] の各サイトに対して、デフォルトで [Rollback] オプションが表示されます。次のいずれかを実行して、各デバイスのエラー状態を解決します。

- ロールバック コマンドを実行するには、[Deploy] をクリックします。
- ロールバック コマンドを変更するには、ウィンドウに表示されるロールバック コマンドを編集し、[Deploy] をクリックします。この操作はカスタム設定の保存されているバージョンには影響しません。
- カスタム設定コマンドを変更して再度実行するには、[Actual] をクリックして実行に失敗したコマンドを表示し、そのコマンドを編集してから、[Deploy] をクリックして編集済みコマンドを実行します。この操作はカスタム設定の保存されているバージョンには影響しません。
- 以降のコマンドの実行をスキップして、デバイスの [Failure] ステータスを解除するには、[Ignore/Reset] をクリックします。

カスタム設定に関する制限事項

カスタム設定機能には以下の制限があります。

- IWAN でプロビジョニングされたデバイスのみがサポートされます。
- 保存するカスタム設定テンプレート名の最大文字数:20
- 1つのカスタム設定テンプレートに保存するコマンド([Actual]コマンドと[Rollback]コマンド)は、9000文字以内でなければなりません。
- デバイスごとに指定できる「パラメータ」(構文:\$<parameter-name>)の最大数:10
- カスタム設定を同時に実行できるデバイスの最大数:20
- デバイスに新しい設定コマンドをプッシュしても、新しい設定はデータベースと自動的に同期されません。その結果、IWAN アプリによってプッシュされた設定と競合する設定は、アプリからプロビジョニング後(N日目)の操作が実行されると上書きされます。
- カスタム設定を作成した後、設定を編集することはできません。変更が必要な場合、既存の設定からテキストをコピーして新しい設定を作成し、それをテキストに貼り付けます。

ハブデバイスの交換

ハブサイト上でプロビジョニングされたデバイス(N日目)を交換することができます。これには、新しいルータが交換前のルータとまったく同様に動作することを確認する目的があります。これは一般に「RMA」と呼ばれます。この手順はブランチサイトのデバイスには適用されません。

手順

-
- 手順 1** 既存のルータ(交換前)へのコンソール接続を使用して、ルータに保存されている実行コンフィギュレーション(running-config)のコピーを作成します。このコピーされた running-config を後の手順で使用するために保存します。
- 手順 2** 交換前のルータを切断します。
- 手順 3** 前のルータが取り付けられていたとおりに新しいルータを接続します。

- 手順 4** 新しく取り付けられたルータへのコンソール接続を使用して、(前の手順で)古いルータからコピーした実行コンフィギュレーションを貼り付けます。
- 手順 5** (Telnet ではなく SSH がデバイスの発見に使用される場合)新しいルータへの SSH アクセスを有効にし、RSA キーとターミナル VTY 回線を作成します。
- 設定モードで、新しいデバイスに次の手順を実行します。

```
ip ssh rsa keypair-name sshkeys
```

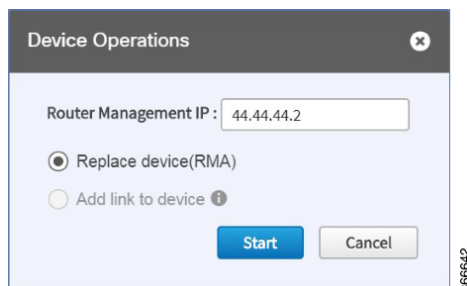
```
! ルータでローカルおよびリモート認証を行う SSH サーバをイネーブルにします。
! SSH バージョン 2 では、絶対サイズは 1024 ビット以上である必要があります。
crypto key generate rsa usage-keys label sshkeys modulus 1024
```

```
! ルータに SSH 制御変数を設定します。
ip ssh time-out 120
```

```
! configure SSH version 2 (will disable SSH version 1)
ip ssh version 2
```

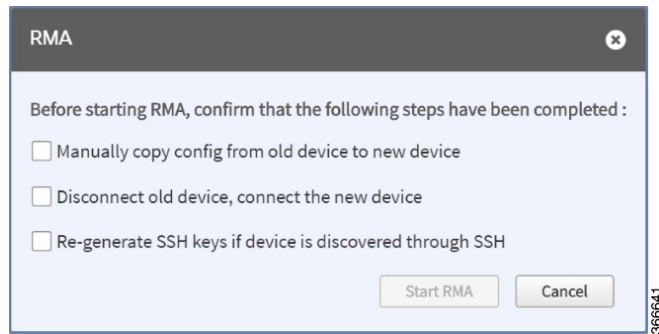
```
!--- Enable SSH
line vty 0 15
transport input telnet ssh
```

- 手順 6** IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。
- 手順 7** [IWAN Aggregation Site] タブをクリックします。ハブ トポロジが表示されます。
- 手順 8** 交換するデバイス(ルータ)をクリックします。[Device Operations] ダイアログボックスが表示されます。



- 手順 9** [Device Operations] ダイアログボックスで、[Replace Device (RMA)] を選択し、[Start] ボタンをクリックします。

ダイアログボックスが表示され、デバイスを交換する前に必要な作業のチェックリストが示されます。次にシステムはインベントリ収集を実行し、古いトラストポイントを削除し、新しいトラストポイントを作成します。



- 手順 10** プロセスを完了できない場合は、問題を説明するメッセージが表示されます。
- 接続の問題がある場合、接続の問題を修復し、[Retry] ボタンをクリックします。
 - 手順がトラブルシューティングの努力にもかかわらず失敗した場合には、[Delete Device] ボタンをクリックします。
- 手順 11** (オプション) 古いルータでスポークが設定され、ルータに接続されている場合、DMVPN トンネルが機能することを確認します。

