CHAPTER 6

Managing Devices

This chapter contains the following sections:

Overview

Each hub site or branch site may have one or more associated devices. The IWAN app provides methods for managing the devices individually, including the Custom Configuration feature, which enables executing batch CLI commands on devices in the network.

Custom Configuration of Devices

Custom Configuration is a mechanism for executing CLI configuration commands on devices within the IWAN network. The feature works similarly to executing a batch file of commands, but operates remotely from the IWAN app. Enter a set of commands (and optionally save them for later use), and select the devices on which to execute the configuration commands. The IWAN app sends the commands to each selected device and then indicates whether execution was successful or not.

Rollback Mechanism in Case of Command Failure

If the command execution is not successful, the feature provides a mechanism for rollback—executing a set of commands to reverse any failed configuration operations.

Per-device Parameters

Custom Configuration provides a “parameter” feature that prompts you at run-time to enter parameter values specific to each device on which the commands are being executed. When you execute the configuration, the system prompts you to enter values one-by-one for each selected target device. Parameters appear as a dollar sign ($) followed by a parameter name.
Example: $interface.

A maximum of 10 parameters may be used.

Custom Configuration Default Templates

The IWAN App includes default configuration templates that provide CLI-level support for various network features. Each template consists of a set of CLI commands to perform a pre-defined function. The templates may include “per-device parameters”—when you execute the configuration, the system prompts you to enter values for the parameters, one-by-one for each selected target device.

The following table summarizes the configuration templates included by default.

Table 6-1 Custom Configuration Default Templates

Template	Description
Liveaction-flow	Enables LiveAction network monitoring. Configures a NetFlow monitor compatible with LiveAction and configures the monitor to export to the LiveAction Server. Choose one of the following templates: • LiveAction-SR1L –Single router with 1 WAN link • LiveAction SR2L – Single router with 2 WAN links • LiveAction SR3L – Single router with 3 WAN links
	The following input is required when executing the template: • LIVEACTION_IP- IP: Address of the LiveAction server. Example: 10.1.0.10 • TUN_INTERFACE: Name of the DMVPN tunnel interface. Example: Tunnel10
Direct Internet Access	Configures Direct Internet Access (DIA). Configures NAT, zone-based policy firewall (ZFW) and Policy-Based Routing (PBR) for Direct Internet Access from a branch. The template also configures tracking of the Internet Gateway IP and failover to Tunnel Overlay if the Internet Gateway is not reachable. **Note** DIA configuration templates are applicable only for Cisco ISR 4000 series routers.
	The following input is required when executing the template: • LAN_SUBNET: Subnet address for LAN with wildcard mask. Example: 10.1.0.0 0.0.255.255 • INET_WAN_INTERFACE_NAME: Internet WAN interface name. Example: GigabitEthernet 0/0/0 • INET_VRF_NAME: Name of the FVRF applied on the WAN interface. Example: IWAN-TRANSPORT-2 • INET_GW_IP: IP address of the internet gateway. Example: 70.70.70.2 • LAN_INTERFACE_NAME: LAN Interface name. Example: GigabitEthernet0/0/2

Table 6-1 Custom Configuration Default Templates

Template	Description
Guest Internet Access	Enables guest internet access on an IWAN branch router. Creates a guest VLAN interface on the router with NAT and zone-based policy firewall (ZFW). The guest VLAN is assigned to a separate VRF called IWAN-GUEST.
	The following input is required when executing the template: • INET_WAN_INTERFACE_NAME: Internet WAN interface name. Example: GigabitEthernet 0/0/0 • INET _GW_IP: IP address of the internet gateway. Example: 70.70.70.2 • GUEST_SUBNET: Subnet address of the Guest VLAN with wildcard mask. Example: 10.2.10.0 0.0.0.255 • GUEST_INTERFACE_NAME: Sub-interface name used for Guest VLAN. Example: GigabitEthernet 0/0/0.66 • GUEST_VLAN_ID: VLAN ID number for Guest VLAN. Example: 66 • GUEST_INTERFACE_IP: IP address for the Guest VLAN interface with mask. Example: 10.1.10.1 255.255.255.0 • GUEST_MASK: Subnet mask used for the Guest VLAN interface. Example: 255.255.255.0

Enabling Custom Configuration

Use the following procedure to enable execution of CLI configuration commands using the Custom Configuration feature.

Procedure

Step 1 On the site list page, display the Custom Config Status column by clicking the gear icon above the table and selecting **Custom Config Status**. The column is displayed and the **Custom Config** button appears above the table.

Creating and Executing a Custom Configuration

Use the following procedure to open the Custom Configuration window to create a Custom Configuration CLI batch file, or to execute an existing Custom Configuration, called a template.

Procedure

Step 1 On the site list page, click the **Custom Config** button above the table. If the button is not displayed, see Enabling Custom Configuration, page 6-3. The Custom Config page appears.

Step 2 Select an existing custom configuration or click the plus-sign icon (+) to create a new one.

Step 3 In the Actual pane, enter the CLI commands to execute, similarly to a batch CLI command file. The commands will be executed in configuration mode on the device.

Note The IWAN app does not perform any validation of the entered commands.

Step 4 (Optional) The full set of commands will be executed on all selected devices. To individually enter parameters specific to each device on which the configuration commands are being executed, use a "parameter" value in the CLI command: a dollar sign ($) followed by a parameter name.
Example: $interface.

When you execute the custom configuration, you will be prompted to enter values for this "parameter" one-by-one for each selected target device. A maximum of 10 parameters may be used.

Step 5 In the Rollback pane, enter the commands to execute in case one or more of the configuration commands in the Actual pane fail to execute correctly. For information about handling failed executions of custom configuration commands, see Handling Failed Custom Configuration Executions, page 6-4.

Step 6 In the Devices pane, select the devices on which to execute the CLI configuration commands.

Step 7 Click **Save** to save the configuration without executing. Click **Deploy** to execute the configuration on the specified devices. The site list page opens automatically, enabling you to view the **Success** or **Failure** status of execution of the configuration commands.

Viewing Status of Custom Configuration Execution

On the site list page, the Custom Config Status column shows the Success or Failure status of execution of the configuration commands per site.

If execution fails for any device within a site, the Custom Config Status column for the site displays **Failure**. If a failure occurs, click the **Failure** link in the Custom Config Status column to display the status of each device within the site. For information about handling failed executions of custom configurations, see Handling Failed Custom Configuration Executions, page 6-4.

Handling Failed Custom Configuration Executions

Use the following procedure to handle failed Custom Configuration CLI command execution.

Procedure

Step 1 On the site list page, the Custom Config Status column shows the **Success** or **Failure** status of execution of the configuration commands per site. If execution fails for any device within a site, the Custom Config Status column for the site displays **Failure**. If a failure occurs, click the **Failure** link in the Custom Config Status column to open a Site Details pop-up.

Step 2 The Site Details pop-up displays the status of each device within the site. For each site with **Failure** status, the Rollback option is displayed by default. Do one of the following to resolve the failure status for each device:

- To execute the rollback command(s), click **Deploy**.
- To change the rollback commands, edit the rollback commands displayed in the window and click **Deploy**. This does not affect the saved version of the custom configuration.
- To change the custom configuration commands and attempt to execute them again, click **Actual** to display the commands that failed to execute, edit the commands, and click **Deploy** to execute the edited commands. This does not affect the saved version of the custom configuration.
- To skip any further command execution and remove the **Failure** status for the device, click **Ignore/Reset**.

Limitations of Custom Configuration

The Custom Configuration feature has the following limitations:

- Only IWAN provisioned devices are supported.
- Maximum number of characters for a saved Custom Configuration template name: 20
- The commands stored in a single Custom Configuration template ("Actual" commands and "Rollback" commands) must not exceed 9000 characters.
- Maximum number of per-device specified "parameters" (syntax: **$<parameter-name>**): 10
- Maximum number of devices on which to execute a Custom Configuration at once: 20
- Pushing a new set of configuration commands to a device does not automatically synchronize the new configuration back to the database. Consequently, any configuration that conflicts with the configuration that is pushed by the prescriptive IWAN app will be overwritten upon execution of the day N operation from the app.
- After creating a custom configuration, it is not possible to edit the configuration. If changes are necessary, copy the text from the existing configuration, create a new configuration, and paste in the text.

Manual Replacement of a Hub Device

Replacing a provisioned device on a hub site requires a manual procedure of several steps. The object is to ensure that the replacement router operates exactly like the router that has been replaced. This is often called “Manual RMA.” This procedure does not apply to devices at branch sites.

Procedure

Step 1 Using a console connection to the existing router (the one being replaced), make a copy of the running configuration (running-config) stored on the router.

a. If the running-config includes “crypto pki trustpoint sdn-network-infra-iwan,” omit this line from the copied text. Do not include this line when pasting the running-config into the replacement router.

b. Save this copied running-config for a later step.

Step 2 Disconnect the router to be replaced.

Step 3 Connect the new router exactly as the previous router was installed.

Step 4 Using a console connection to the newly installed router, paste in the running configuration that was copied (in an earlier step) from the old router.

Step 5 Enable SSH access to the new router, creating RSA keys and terminal VTY lines.

Step 6 Wait for the APIC-EM inventory sync to occur automatically. This typically occurs within 25 minutes.

To verify that the inventory sync has occured for the new router:

a. On the new router, use the **show version** command to display the serial number.

b. Open the Device Inventory app in APIC-EM. A table displays all devices in the IWAN network.

c. Using the Layout menu, ensure that the table displays serial numbers.

d. Verify that the serial number of the new router is displayed, and that the “Last Inventory Collection Status” column indicates “Managed” for the new router.

Step 7 Create a trustpoint for the new router by executing API commands through APIC-EM.

a. On the new router, enter the **show license udi** command.

b. Make note of the platform ID (PID column). Example: ASR1002-X

c. Open the APIC-EM home page and click “API” in the menu bar at the top. APIC-EM displays a list of available APIs.

d. In the list of APIs, click “PKI Broker Service”. Click “Show” to display the PKI Broker Service REST API command options.

e. Click **POST /trust-point**.

f. In a text editor, assemble the following information for the new router, in JSON format as shown below:

```
{
"entityName": "host-name",
"platformId": "platform-ID",
"serialNumber": "serial-number",
"trustProfileName": "sdn-network-infra-iwan",
"entityType": "router"
}
```

Example:

```
{
"entityName": "acdc01rou001.iwanserver.com",
"platformId": "ASR1001-X",
"serialNumber": "FXS1234Q5J6",
"trustProfileName": "sdn-network-infra-iwan",
"entityType": "router"
}
```

Table 6-2 New Router Information for Adding Trustpoint

Field	Value
entityName	Hostname of the new router. It is recommended to use the same hostname as the previous router being replaced.
platformId	Platform-ID displayed by the **show license udi** command (described in a previous step).
serialNumber	Serial number of the new router. The serial number is displayed using the **show version** command (described in a previous step).
trustProfileName	Value: sdn-network-infra-iwan
entityType	Value: router

g. In the pkiTrustPointInput field, paste in the information collected in the previous step, in JSON format.

h. In the APIC-EM window, click **GET /trust-point**.

i. Click the **Try it out** button.

j. Scroll to the bottom of the Response Body text and copy the value of the “id” field.

Example: "id": "efb1234d-0123-456d-bd12-345a12345b67"

k. In the APIC-EM window, click **POST /trust-point/{trustPointId}**.

l. In the Parameters section, for the trustPointId parameter, paste in the value copied from the response text of the previous API command.

Example: efb1234d-0123-456d-bd12-345a12345b67

Step 8 On the new router, in config mode, enter the following commands to add a CLI command to the ikev2 profile:

crypto ikev2 profile <*profile-name*>

pki trustpoint sdn-network-infra-iwan

Example:

```
Router(config)#crypto ikev2 profile FVRF-IKEv2-IWAN-TRANSPORT-4
Router(config-ikev2-profile)# pki trustpoint sdn-network-infra-iwan
```

Step 9 (Optional) If the old router had spokes configured and connected to the router, verify that the DMVPN tunnels are operational.