Brownfield Validation Messages

This chapter contains the following sections:

Adding Greenfield and Brownfield Devices to Cisco IWAN

The Cisco IWAN application (IWAN app) can add “greenfield” or “brownfield” devices to the IWAN network.

“Greenfield” refers to new, unconfigured devices. Because these devices do not have any pre-existing configuration, there are no conflicts when bringing them into the IWAN network and configuring them using the IWAN app.

“Brownfield” refers to devices that belong to existing sites that are being added to an IWAN network. They may have pre-existing configurations to synchronize with IWAN-based configuration, and these existing configurations may cause conflicts.

Validation

While provisioning a brownfield device, the IWAN app performs a validation to determine whether any configuration conflicts exist. It reports the conflicts in two categories:

- Errors—Conflicts that prevent adding the device to the IWAN network.
- Warnings—Conflicts that do not prevent the device from being added to the IWAN network. It is recommended to correct the configuration issues that trigger validation warnings.

If the IWAN app detects an error or warning during provisioning, correct the issue on the device and perform the validation again. Refer to the Errors and Warnings sections below for details.

Errors

The following table describes errors that can occur during validation. These errors prevent adding a device to the IWAN network.

Table A-1 Validation Errors

Configuration Conflict	Recommendation
Username configuration must have privilege level 15.	Configure a username with privilege level 15 on the device. **Example:** **username** *username* **privilege 15 password 0** *password*
PfR configuration must not be present on the device.	Ensure that Performance Routing (PfR) configuration is not present on the device. **Example:** **no domain ONE**
QoS configuration must not be present on the device.	Ensure that Quality of Service (QoS) configuration is not present on the device. **Example:** **no class-map match-any nbar-12-cls#VOICE** **no policy-map nbar-12-cls** **no policy-map IWAN-INTERFACE-SHAPE-ONLY-INTERNET** **no service-policy input nbar-12-cls** **no service-policy output IWAN-INTERFACE-SHAPE-ONLY-INTERNET**
Interface loopback 47233 must not be configured on the device.	Remove interface loopback 47233 from the device. **Example:** **no interface loopback47233**
IWAN trustpoint configuration must not be present on device.	Remove Cisco IWAN trustpoint configuration from the device. **Example:** **no crypto pki trustpoint sdn-network-infra-iwan**
VPN routing and forwarding (VRF) configuration must not be present on the device.	Remove the existing VRFs as VRFs as it will interfere with the Cisco IWAN configuration. Make sure that the routers do not have any of the following VRFs: • IWAN-TRANSPORT-1 • IWAN-TRANSPORT-2 • IWAN-TRANSPORT-3 • IWAN-TRANSPORT-4 **Example:** **no ip vrf IWAN-TRANSPORT-4**

Table A-1 Validation Errors

Configuration Conflict	Recommendation
Recovery configuration file unavailable in flash	IWAN recovery configuration file "IWAN_RECOVERY.cfg" is needed to enable recovery of device. Create a recovery file using the CLI command: **copy running-config flash:IWAN_RECOVERY.cfg**
Conflicting EIGRP configuration present on the device	Remove EIGRP configuration using the CLI command: **no router eigrp IWAN-EIGRP**
Configure Port-Channel in aggregate mode to support QoS policy configuration	Applicable only to ASR routers. Ensure that port-channel is in aggregate mode when it is used as WAN/LAN interface. Configure port-channel aggregate mode using the CLI command: **platform qos port-channel-aggregate <port-channel-number>**
QoS policy configuration is not supported for the targeted type of interface: Port-Channel	Device platform type does not support QoS policy configuration on port-channel interface. Choose other types of LAN/WAN interface.

Warnings

The following table describes errors that can occur during validation. These warnings do not prevent a device from being added to the IWAN network, but it is recommended to correct the issues that trigger these warnings.

Table A-2 Validation Warnings

Configuration Conflict	Recommendation
Please make sure at least two interfaces for WAN and LAN are up and running.	Ensure that the two interfaces for WAN and LAN are up and running. Verify using the **show ip interface brief** command.
IWAN related crypto configuration found on the device.	Remove the crypto configuration because the crypto configuration might interfere with the Cisco IWAN configuration. **Example:** `crypto zeroize mypubkey rsa sdn-network-infra-iwan`
No routing protocol found on device.	Enable one of the following routing protocols on the device. **Example:** `router ospf` *AS number* `router eigrp` *AS number* `router bgp` *AS number*

EZPM configuration found on the device.	Remove Easy Performance Monitor (EZPM) configuration as EZPM configuration might interfere with the Cisco IWAN configuration.
	Example:
	`no class-map match-all Business-Critical-and-default-tcp-only`
	`no performance monitor context IWAN-Context profile application-experience`

Table A-2 Validation Warnings

Configuration Conflict	Recommendation

NBAR configuration found on the device.	Remove the Network Based Application Recognition (NBAR) configuration as NBAR configuration might interfere with the Cisco IWAN configuration.
	
	Example:
	`no ip nbar attribute-map Consumer_App_Prof`
	`no ip nbar attribute-map Other_Custom`
	`no ip nbar attribute-map Net_Admin_Custom`

No device information available for validation.	Revalidate and if problem persists, ensure the following: • Device is up and running. • Device connectivity is established.
Device does not have valid image version and K9 package.	The Cisco IWAN app does not support the Cisco software image loaded on the device. Boot the device with a 15.5(3) or 15.5(4) image with the K9 feature pack. **Example:** `asr1000rp1-adventerprisek9.03.16.00.S.155-3.S-ext.bin`
Insufficient number of VTY lines present on the device	A minimum of 16 VTY lines are required to be configured on the device. **line vty <first-line-number> <last-line-number>**
One of the VTY line exec-timeout is less than 5 mins	Ensure VTY line exec timeout are not less than 5 minutes Verify using the CLI command: **show running-config | sec line vty**
Configured Throughput on device does not match with installed license throughput	Applicable only to CSR routers. Remove the **platform hardware throughput level** CLI to achieve maximum throughput, as follows: **no platform hardware throughput level MB <configured-value>**
No active license found on the device	Applicable only to CSR routers. Either the license has expired or is not supported. Verify license issues using CLI command: **show self-diagnostics**
Device does not have required license.	Required licenses are not enabled on the device. Enable the licenses for the platform in use. • ASR routers: adventerprisek9 or advipservicesk9 and IPSEC EULA should be accepted • ISR 4000 Series routers: appxk9 and securityk9 • ISR G2 routers: datak9 and securityk9 • CSR routers: ax
Device clock is not synchronized	Ensure that the router clock is in sync with controller clock. Verify using the **show clock** command. Recommended to configure NTP server using the CLI command: **ntp server <controller-ip>**