Release Notes for Cisco Configuration Professional Express 3.5.3

First Published: September 25, 2018

This Release Notes document supports Cisco Configuration Professional Express Release 3.5.3. This document should be used with the documents listed in the "Related Documentation" section on page 24.

This Release Notes is updated as required. To ensure that you have the latest version of the Release Notes, go to http://www.cisco.com/en/US/products/ps9422/tsd_products_support_series_home.html. In the Support area, choose **Software Downloads, Release and General Information > Release Notes**, and locate the release notes pertaining to your release.

Contents

This document contains the following sections:

Cisco Systems, Inc.
www.cisco.com

Introduction

Cisco Configuration Professional Express is an embedded, device-management tool that enables bootstrap configuration and provisioning of an Cisco Integrated Services Router (ISR).

CCP Express provides you two options to bring up a brand new router. You can use the Quick Setup Wizard to perform the basic configuration tasks and Advanced Setup option for detailed configuration options. For a brand new router Quick setup wizard is the preferred option.

Supported Routers

Table 1lists the routers that Cisco Configuration Professional Express supports.

Table 1   Supported Routers

Router Series	Supported Routers
Cisco 800M Series	C841M-4X/K9R-K9
	C841M-4X/K9R-NPEK9
	C841M-8X/K9R-K9
	C841M-8X/K9R-NPEK9
	C841M-8X-JAIS/K9
	C841M-4X-JAIS/K9
	C841M-4X-JSEC/K9
Cisco 812 Series	C812G+7-K9
	C812G-CIFI+7-E-K9
	C812G-CIFI+7-N-K9
	C812G-CIFI-V-A-K9
	C812G-CIFI-S-A-K9
Cisco 815 Series	CISCO815
	CISCO815-VPN-K9

Table 1   *Supported Routers (continued)*

Router Series	Supported Routers
Cisco 819 Series	C819HGW+7-E-K9
	C819HGW+7-N-K9
	C819HGW+7-A-A-K9
	C819HGW-V-A-K9
	C819HGW-S-A-K9
	C819H-K9
	C819HG-U-K9
	C819HWD-E-K9
	C819HWD-A-K9
	C819HG-4G-V-K9
	C819HG-4G-A-K9
	C819HG-4G-G-K9
	C819G-4G-V-K9
	C819G-4G-A-K9
	C819G-4G-G-K9

Table 1 **Supported Routers (continued)**

Router Series	Supported Routers
Cisco IR 829 Series	IR829GW-LTE-LA-NK9
	IR829GW-LTE-GA-SK9
	IR829GW-LTE-GA-CK9
	IR829GW-LTE-GA-ZK9
	IR829GW-LTE-GA-EK9
	IR829GW-LTE-NA-AK9
	IR829GW-LTE-VZ-AK9
	IR829B-LTE-EA-AK9
	IR829B-LTE-EA-BK9
	IR829B-LTE-EA-EK9
	IR829M-2LTE-EA-AK9
	IR829M-2LTE-EA-BK9
	IR829M-2LTE-EA-EK9
	IR829M-LTE-EA-AK9
	IR829M-LTE-EA-BK9
	IR829M-LTE-EA-EK9
	IR829M-LTE-LA-ZK9
	IR829B-2LTE-EA-BK9
	IR829B-2LTE-EA-EK9
	IR829B-2LTE-EA-AK9
	IR829B-LTE-LA-ZK9
Cisco IR 809 Series	IR809G-LTE-VZ-K9
	IR809G-LTE-NA-K9
	IR809G-LTE-GA-K9
	IR809G-LTE-LA-K9
Cisco IR 807	IR807G-LTE-GA-K9
	IR807G-LTE-NA-K9
	IR807G-LTE-VZ-K9
Cisco 857 Series	CISCO857-K9
	CISCO857W-G-A-K9
	CISCO857W-G-E-K9
Cisco 861 Series	CISCO861-K9
	CISCO861W-GN-A-K9
	CISCO861W-GN-E-K9
	CISCO861W-GN-P-K9

Table 1 **Supported Routers (continued)**

Router Series	Supported Routers
Cisco 866 Series	CISCO866VAE-W-E-K9
Cisco 867 Series	CISCO867VAE-K9
	CISCO867-K9
	CISCO867VA-K9
	CISCO867W-GN-A-K9
	CISCO867W-GN-E-K9
	CISCO867VAE-W-A-K9
	CISCO867VAE-W-E-K9
	CISCO867VAE-POE-W-A-K9
Cisco 871 Series	CISCO871-K9
	CISCO871W-G-A-K9
	CISCO871W-G-E-K9
	CISCO871W-G-J-K9
Cisco 876 Series	CISCO876-K9
	CISCO876W-G-E-K9
Cisco 877 Series	CISCO877-K9
	CISCO877-M-K9
	CISCO877W-G-A-K9
	CISCO877W-G-E-K9
	CISCO877W-G-E-M-K9
Cisco 878 Series	CISCO878-K9
	CISCO878W-G-A-K9
	CISCO878W-G-E-K9

Table 1   *Supported Routers (continued)*

Router Series	Supported Routers
Cisco 881 Series	CISCO881-K9
	CISCO881-PCI-K9
	CISCO881-SEC-K9
	C881W-A-K9
	C881W-P-K9
	C881-V-K9
	C881GW+7-A-K9
	C881GW+7-E-K9
	C881GW-S-A-K9
	C881GW-V-A-K9
	C881WD-A-K9
	C881WD-E-K9
	CISCO881W-GN-A-K9
	CISCO881W-GN-E-K9
	CISCO881W-GN-P-K9
	CISCO881W-A-K9
	CISCO881W-E-K9
	CISCO881G-K9
	CISCO881GW-GN-A-K9
	CISCO881GW-GN-E-K9
	CISCO881G-S-K9
	CISCO881G-V-K9
	CISCO881G-A-K9
	C881G-U-K9
	C881G-S-K9
	C881G-V-K9
	C881G-B-K9
	C881G+7-K9
	C881G+7-A-K9
	C881SRST-K9
	C881SRSTW-GN-A-K9
	C881SRSTW-GN-E-K9
	C881-K9

Table 1　　　*Supported Routers (continued)*

Router Series	Supported Routers
Cisco 886 Series	CISCO886-K9
	CISCO886G-K9
	CISCO886VA-K9
	C886VA-W-E-K9
	C886VAG+7-K9
	CISCO886GW-GN-E-K9
Cisco 887 Series	C887VA-V-K9
	C887VA-W-A-K9
	C887VAG-S-K9
	C887VAGW+7-A-K9
	C887VAGW+7-E-K9
	C887VA-WD-A-K9
	C887VA-WD-E-K9
	CISCO887-K9
	CISCO887VA-K9
	CISCO887VA-M-K9
	C887VA-W-A-K9
	C887VA-W-E-K9
	C887VAM-W-E-K9
	C887VAG-S-K9
	C887VAG+7-K9
	C887VAMG+7-K9
	CISCO887W-GN-A-K9
	CISCO887W-GN-E-K9
	CISCO887M-K9
	CISCO887MW-GN-E-K9
	CISCO887G-K9
	CISCO887GW-GN-A-K9
	CISCO887GW-GN-E-K9
	CISCO887V-K9
	CISCO887VW-GNA-K9
	CISCO887VW-GNE-K9
	CISCO887VG-K9
	CISCO887VGW-GNA-K9
	CISCO887VGW-GNE-K9

Table 1 **Supported Routers (continued)**

Router Series	Supported Routers
Cisco 888 Series	CISCO888-K9
	CISCO888-SEC-K9
	CISCO888W-GN-E-K9
	CISCO888E-K9
	CISCO888EW-GNE-K9
	C888EA-K9
	C888SRST-K9
	C888ESRST-K9
	C888ESRSTW-GNA-K9
	C888ESRSTW-GNE-K9
	CISCO888-K9
	CISCO888W-GN-A-K9
	CISCO888W-GN-E-K9
	CISCO888E-K9
	CISCO888EW-GN-A-K9
	CISCO888EW-GN-E-K9
	CISCO888G-K9
	CISCO888GW-G-NA-K9
	CISCO888GW-G-NE-K9
	C888EG+7-K9
	C888SRST-K9
	C888SRSTW-GN-A-K9
	C888SRSTW-GN-E-K9
Cisco 891 Series	CISCO891W-AGN-A-K9
	CISCO891W-AGN-C-K9
	CISCO891W-AGN-N-K9
	CISCO891-K9
	C891F-K9
	C891FJ-K9
	CISCO891-24X/K9
	C891-24X/K9

Table 1 **Supported Routers (continued)**

Router Series	Supported Routers
Cisco 892 Series	CISCO892J-K9
	CISCO892FW-A-K9
	CISCO892W-AGN-P-K9
	C892FSP-K9
	CISCO892-K9
	CISCO892F-K9
	CISCO892W-AGN-E-K9
Cisco 896	C896VA-K9
Cisco 897	C897VA-K9
	C897VAW-A-K9
	C897VAW-E-K9
	C897VA-M-K9
	C897VAM-W-E-K9
Cisco 898	C898EA-K9
Cisco 900 series	C921-4P
	C921J-4P
	C931J-4P
	C931-4P
	C941J-4P
	C927-4P
	C927-4PM
	C926-4P
	C921-4PLTEGB
	C921-4PLTEAU
	C921-4PLTEAS
	C927-4PLTEGB
	C927-4PLTEAU
	C927-4PMLTEGB
	C926-4PLTEGB

Table 1   *Supported Routers (continued)*

Router Series	Supported Routers
Cisco 1801	CISCO1801
	CISCO1801/K9
	CISCO1801-M
	CISCO1801-M/K9
	CISCO1801W-AG-B/K9
	CISCO1801W-AG-C/K9
	CISCO1801W-AG-N/K9
	CISCO1801WM-AGB/K9
Cisco 1802	CISCO1802
	CISCO1802/K9
Cisco 1803	CISCO1803/K9
	CISCO1803W-AG-B/K9
	CISCO1803W-AG-E/K9
Cisco 1805	CISCO1805-D
	CISCO1805-D/K9
	CISCO1805-EJ
Cisco 1811	CISCO1811/K9
	CISCO1811W-AG-B/K9
	CISCO1811W-AG-C/K9
	CISCO1811W-AG-N/K9
Cisco 1812	CISCO1812/K9
	CISCO1812-J/K9
	CISCO1812 W-AG-C/K9
	CISCO1812W-AG-P/K9
Cisco 1841	CISCO1841

Table 1   *Supported Routers (continued)*

Router Series	Supported Routers
Cisco 1861	CISCO1861-SRST-B/K9
	CISCO1861-SRST-C-B/K9
	CISCO1861-SRST-C-F/K9
	CISCO1861-SRST-F/K9
	CISCO1861-UC-2BRI-K9
	CISCO1861-UC-4FXO-K9
	CISCO1861E-SRST-B/K9
	CISCO1861E-SRST-C-B/K9
	CISCO1861E-SRST-C-F/K9
	CISCO1861E-SRST-F/K9
	CISCO1861E-UC-2BRI-K9
	CISCO1861E-UC-4FXO-K9
	CISCO1861W-SRST-C-B/K9
	CISCO1861W-SRST-C-F/K9
	CISCO1861W-SRST-B/K9
	CISCO1861W-SRST-F/K9
	CISCO1861W-UC-2BRI-K9
	CISCO1861W-UC-4FXO-K9
Cisco 1902	CISCO1902/K9
Cisco 1905	Cisco1905/K9
Cisco 1921	Cisco1921/K9
	Cisco 1921DC/K9
Cisco 1941	Cisco 1941/K9
	Cisco1941W-A/K9
	Cisco1941W-E/K9
	Cisco1941W-P/K9
	Cisco1941W-N/K9
	Cisco1941W-C/K9
Cisco 2800 Series	CISCO2801
	CISCO2811
	CISCO2821
	CISCO2851

Table 1   ***Supported Routers (continued)***

Router Series	Supported Routers
Cisco 2900 Series	CISCO2901/K9
	CISCO2911/K9
	CISCO2921/K9
	CISCO2951/K9
Cisco 3800 Series	CISCO3825
	CISCO3825-NOVPN
	CISCO3845
	CISCO3845-NOVPN
Cisco 3900 Series	CISCO3925/K9
	CISCO3925E/K9
	CISCO3945/K9
	CISCO3945E/K9

Supported HWICs

Table 2 lists the HWICs that Cisco Configuration Professional Express supports.

Table 2   Supported HWICs

HWICs
EHWIC-VA-DSL-A
HWIC-4SHDSL
EHWIC-VA-DSL-M
HWIC-2SHDSL
HWIC-3G-GSM
HWIC-3G-CDMA-V
HWIC-3G-CDMA- Global
HWIC-3G-CDMA-S
EHWIC-3G-EVDO-V
EHWIC-3G-EVDO-B
EHWIC-3G-HSPA+7
EHWIC-4G-LTE-V
WIM-4G–LTE (For Nano Only)

Supported Browsers

Cisco Configuration Professional Express is supported on the following browsers:

- Google Chrome (Version 30.x to 68.0.x)
- Mozilla Firefox (Version 25.x to 62.0.x)
- Safari 9.1

Cisco IOS Releases

Cisco Configuration Professional Express requires Cisco IOS Release 15.2.4M2 or later, or Release 15.3.1T or later for all SKUs. To get all security features support use the release 15.5(1)T. For CCP Express 3.5.3, it is recommended to use IOS release 15.7(3)M2.

Determining the Cisco IOS Release

To determine the Cisco IOS software release currently running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the Cisco IOS release in the second line.

```
Router> show version
c3845-1# show version
```

```
Cisco IOS Software, 3800 Software (C3845-ADVENTERPRISEK9-M), Version 12.4(11)XW2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 03-Jul-07 00:49 by prod_rel_team
```

Installation Files

The Cisco Configuration Professional Express 3.5.3 installation files are left untarred on the router flash.

What is New in Release 3.5.3

Release 3.5.3 introduces the following new features and bug fixes:

- Support for 4G LTE module (WIM-4G-LTE) in Nano (841M series)
- Support for Cisco 900 Series (Viper) routers
- Support for 4 IR829 series routers - IR829B-2LTE-EA-BK9, IR829B-2LTE-EA-EK9, IR829B-2LTE-EA-AK9, IR829B-LTE-LA-ZK9

What is Not Supported in Release 3.5.3

Release 3.5.3 does not support the following features:

- Microsoft Edge browser support is not present in 3.5.1 (carried on from 3.5 onwards).
- AVC feature is not supported on IR routers (IR8x9 and IR8x7 series devices).
- IpSec VPN is not supported on IR routers (IR8x9 and IR8x7 series devices).

Known Issues and Workarounds

This following is the list of known issues in Cisco Configuration Professional Express Release 3.5.3:

- CSCtz82923

  Symptom: In the Interface screen (in both the Admin view and the EndUser view), the Edit VLAN and Edit Interface dialog boxes do not reflect the correct values for the attributes displayed on the Summary screen.

  Condition: This issue occurs when the Interfaces feature is in use, and an interface or a VLAN is being edited.

  Workaround: Upgrade your Cisco IOS Software Release to 15.2(4)M or later.

- CSCud76752

  Symptom: The Cisco Configuration Professional Express interfaces screen displays a blank page.

  Condition: This issue occurs when the Cisco IOS Release that is being used is earlier than Release 15.2, and router has cellular interfaces.

  Workaround: Upgrade to Cisco IOS Release 15.2.4M2 or later, or Release 15.3.1T or later for all SKUs.

- CSCup66372

    Symptom: While creating a user very first time in a new router the password is not encrypted..

    Condition: The user will be prompted to create a new user while logging in to the router for the first time with default username and password. The newly created user is not encrypted. The password will be visible when anyone tries to check the running configuration.

    Workaround: Login to router and execute a CLI "service password-encryption" in config mode. Otherwise navigate to "Configure CLI" menu and execute the same CLI in config mode.

- CSCus23237

    Symptom: NAT translations do not happen if stale NAT translation CLIs present in the configuration.

    Condition: This problem is seen when interface enabled for NAT feature is deleted using CCP Express 3.0 [on supported Cisco Routers]

    This problem occurs with the following conditions:

    1. Enabling NAT during Interface configuration and deleting it

    2. Configuring an interface as Primary WAN interface and deleting it

    3. Configuring an interface as Secondary WAN interface and deleting it

    In above conditions following CLIs are sent to router from CCPExpress software and stays in configuration as stale entries when deleted

    ```
    ! //**** Below CLI sent as part of interface configuration enabled for NAT**** //
    !
    ip nat inside source list <Nat-list_name> interface <Interface_name> overload
    !
    !//**** Below CLI sent as part of Primary/Secondary WAN interface configuration**** //
    !
    ip nat inside source route-map <route_map_name> interface <Interface_name> overload
    ```

    Workaround:

    1. If the interface part of NAT overload configuration is deleted then create that interface (see example below)

    2. Delete the stale NAT overload CLI

    3. Delete the created interface

    4. Execute "clear nat translations forced"

    Example

    Below entry may exist on the device causing NAT translations to not work properly.

    ```
    !
    ip nat inside source list nat-list interface Dialer4 overload
    !
    Config t
    (config)#int dialer4
    (config-intf)#exit
    (config)# no ip nat inside source list nat-list interface Dialer4 overload
    (config)#exit
    #.
    ```

- CSCuq63961

    Symptom: Unable to access the Internet. Traffic is not going through the configured WAN interface.

Condition: When the WAN interface gets its IP and default gateway from DHCP server, CCP Express should not push "ip route 0.0.0.0 0.0.0.0 'primary WAN interface'" configuration to the router. With this configuration the traffic is not flowing through the device, when already the default route (GW IP received from DHCP server) is installed on the router.

Workaround: Remove the CLI manually in the router like "no ip route 0.0.0.0 0.0.0.0 'primary WAN interface'" or using CCP Express "anyCli" feature to execute the CLI

- CSCuq64556

Symptom: The protocol 914c/g protocol is not listed under net-admin application list in the Policy screen.

Condition: This particular protocol not be configured using CCP Express.

Workaround:

There is no workaround. If we configure "match protocol 914c/g" under any of the class-maps using CLI on the router, then UI will throw "parsing error" while accessing some features eg. CWS

- Cvc63172

Symptom: Uploads in CCP Express are getting aborted automatically under certain conditions in Microsoft Internet Explorer due to browser timeout issues.

Condition: When Microsoft Internet Explorer is used, we have noticed that certain devices shoot up in the CPU utilization to 100%. This causes subsequent processing to halt. The options are to try again or use Google Chrome, Mozilla Firefox, or Microsoft Edge browsers.

Workaround:

There is no workaround for this in Microsoft Internet Explorer.

- CSCvc78268

Symptom: Integration with Cisco Active Advisor works at authentication level, but you cannot upload data from device in Microsoft Internet Explorer.

Condition: When Microsoft Internet Explorer is used, the authentication to CAA works, but the data upload does not work. We need to use Google Chrome, Mozilla Firefox, or Microsoft Edge.

Workaround: There is no workaround for this in Microsoft Internet Explorer.

- CSCvc66233

Symptom: IOS upload not listing the IOS image on the IR boxes.

Condition: The command show file info should yield "type is image" for any IOS image file. In IR routers, this is shown as "ebcdic text". Hence the files are not listed.

Workaround: A code workaround to check for ebcdic text if the box type is IR is put in to list the IOS images. This is entirely not correct as vlan.dat (and also other files which are not known at this point) can also be listed as ebcdic text. So code has excluded vlan.dat from the checks and only checks for type as ebcdic text to list the IOS images. In addition, since IR devices use IOS installation bundles, the file is checked for presence of "bundle" in its name. The user will have to manually identify and select the correct IOS image bundle.

- CSCvc67305

Symptom: Dashboard router option is not showing Hardware Health in IR routers..

Condition: Hardware Health option in Dashboard is not listed. The output of the command "show environment all" given by IOS in IR routers is very much different when compared to the standard output given in ISR routers for IOS (based on which the initial design was done).

Workaround: There is no workaround here. By design, if the values cannot be fetched, the dashlet will not be displayed.

- CSCvc69108

  Symptom: Login to UI is not possible for user with privilege level other than 15.

  Condition: HTTP server in IOS permits only privilege level 15 user credentials to be used for application login.

  Workaround: There is no workaround. User should be created with privilege level.

- CSCvc78268

  Symptom: Integration with Cisco Active Advisor works at authentication level, but you cannot upload data from device in Microsoft Internet Explorer.

  Condition: When Microsoft Internet Explorer is used, the authentication to CAA works, but the data upload does not work. We need to use Google Chrome, Mozilla Firefox, or Microsoft Edge.

  Workaround: There is no workaround for this in Microsoft Internet Explorer.

- CSCvd89365

  Symptom: Upgrade from an older version causes top menu items to launch different pages.

  Condition: When user upgrades to version 3.4 from older versions, the page reloads after the upgrade and clicking the top menu items may launch different pages.

  Workaround: Clear the browser cache and launch CCP Express again. This is because top menu was rearranged and after the installation, the old file is present on the browser and does not fetch the new file.

- CSCvd89987

  Symptom: Safari browser does not do copy to clipboard, download of config and also allow user to enter data in certain fields.

  Condition: Safari browser does not support every element currently used. Blob and Datalist are not supported.

  Workaround: Datalist is used in few pages where the drop down has values and also allows user to enter any value. This option of entering values will not be available when using Safari. Also Copy to Clipboard and Download of config is not displayed in Safari. In case this support is required, user should use any other supported browser.

- CSCve54553

  Symptom: On the IR829 Dual-LTE, controller profile configuration results in unnecessary warning for modem-reset.

  Condition: When pushing the controller configuration from Quick Setup Wizard, the device issues warnings even when the pushed configuration is the existing default.

  Workaround: The fix for this is addressed in CCP Express defect CSCve52052 (Ambiguous instruction to reset modem leads to incomplete workflow). For every profile push, a modem reset is issued from CCP Express in the case of dual LTE. With this fix in the code, the issue of ambiguous instructions displayed to the user leading to configuration breakage is addressed

- CSCve61217

  Symptom: IOX Device Manager does not launch on theIR809.

  Condition: This is caused by a platform bug in IOS 15.6.3M1 release. When IOS is upgraded from 15.6.3M1 to latest 15.6.3M2 the Guest OS product_id is not getting updated with a valid ID and the 'caf' process stops running.

Workaround: To overcome this issue, follow these steps from the Guest OS console.

IR800-GOS-1:~# cp /etc/platform/product_id /software/caf/work/product_id

IR800-GOS-1:~# monit restart caf

Check CAF status by executing 'monit summary'. You should be see caf in a Running state.

After following the above steps, the device will be able to launch the IOX manager UI manually as well as from CCP_Express.

- CSCve48207

  Symptom: Default configuration can cause a device lockout.

  Condition: The default configuration contains a one-time user, which is removed if logged in via telnet.

  Workaround: The default configuration leaves the console without any login credentials. In case of a lockout, the user can always use the console to gain access back to the device. To counter the connectivity issue, the new user is written to the device before the existing one-time user is cleared.

- CSCve00127

  Symptom: Quick Setup Wizards provides an option for WiFi AP Config on the IR829 device, but doesn't actually configure the AP.

  Condition: This happens when the BVI Interface is not configured.

  Workaround: The user has to ensure that BVI IP address is configured before using Wizard WiFi configuration.

- CSCve87173

  Symptom: WiFi configuration not getting pushed on LAN network change.

  Condition: When a user changes the LAN network while using the Quick Setup Wizard, the WiFi configuration gets pushed to the AP. This is followed by a write memory which will save the configuration on the AP. Following this the BVI interface address is updated. But since the network change happened, the AP would not be reachable from 10.10.10.0 network. This means that the change to the BVI Interface IP address is pushed, but is not written to memory. And in case of a reboot or power failure after the day 0 configuration using Quick Setup Wizard, this IP Address change can be lost.

  Workaround: In case of a LAN network change, user should login to the router using the new IP address, session in to AP and then issue a write memory. This will ensure that the changes to BVI interface is saved to memory in the AP

- CSCve77908

  Symptom: IR809 cellular interface configuration not working as expected.

  Condition: Cellular interface profile changes are returning an error on an IR809 running on 15.6(3)M2 IOS.

  Additionally, the modem related information is returned as blank values.

  Workaround: This platform issue for IR809 is addressed in IOS release15.7. The user should upgrade to this latest version, subject to its availability.

- CSCve93346

  Symptom: Performance issue on the IR800 series.

  Condition: The IR800 could display slow performance if the Guest OS is consuming too many CPU resources.

Workaround: Refer to the software configuration guide in the IR800 documentation for examples of performance tuning. This should only be done under the recommendation of Cisco or an authorized partner. 4G performance may be impacted if changed without proper guidelines.

- CSCve93356

    Symptom: Application shows issues when using the Edge Browser. Many elements are not rendered correctly and the user is unable to proceed with actions.

    Condition: Some features of the application are not working when using the Edge Browser as compared to other browsers.

    Workaround: Use any of the following browsers: Chrome, Firefox, Safari (Mac only) and Internet Explorer 11 (Windows only).

- CSCve93367

    Symptom: On the IR809, when security is configured, IOX access via LAN may not work if the right configuration is not present.

    Condition: When security is configured, zones come into effect. So if IOX configuration is done, both the IOX interface as well as the interface acting as the LAN interface should be present in the LAN zone for IOX LAN access to work.

    Workaround: The application cannot check if the interface acting as the LAN interface is present in the LAN zone. The user should navigate to the Zones screen under the Security tab, and add the respective interface under Zone LAN. Once this is done, IOX access via LAN should help the user access the Device Manager.

- CSCvf58395

    Symptom: CPU Graph has a rendering delay when configuration radio options are clicked.

    Condition: User launches Dashboard and clicks on CPU Dashlet link. The dashlet loads and displays the data in graph format. If you change the interval options, the graph takes a couple of seconds to fetch and display the data. This is due to the time taken to query the device and the time for the plug-in to render the graph.

    Workaround: There is no workaround for this.

- CSCvf62728

    Symptom: Modem details are not listed in CCP Express running on IR807 platform.

    Condition: In IR807, Modem details do not get listed. This is because the IOS does not provide the Modem details for the standard command.

    Workaround: There is no workaround for this. User will have to check and upgrade to the version of IOS where the Modem details are listed for IR807.

- CSCvf33726

    Symptom: Upgrade of CCP Express fails in Edge browser.

    Condition: When using Edge for CCP Express upgrade, it is noticed that the upgrade process fails. Sometimes this happens frequently. The options are to try again or use Chrome, or Firefox browsers.

    Workaround: There is no workaround for this in Edge.

- CSCvf44305

    Symptom: Cisco 800 Series ISR does not support some Transform Set combinations in VPN advanced configuration.

    Condition: Some Transform Set combinations give error while doing VPN advanced configurations. The application lists only those transform sets which are available on the platform.

Workaround: User to use discretion while choosing the transform sets. There is no other workaround for this.

- CSCvf68058

  Symptom: Password entered in SNMP configuration is not fetched back by application.

  Condition: IOS does not display the password used in SNMP configuration via any supported command. Since the value cannot be fetched back from the device, this field cannot be populated.

  Workaround: There is no workaround for this as this is purely from the IOS platform.

- CSCvf78050

  Symptom: CCP Express does not defend against CSRF attack.

  Condition: CCP Express application can defend against CSRF attack only if the IOS HTTP server employs a usable solution to fix the same.

  Workaround: There is no workaround for the same.

- CSCvf76911

  Symptom: Safari browser does not list the default ports shown as drop-down for TCP & UDP in extended ACL configuration.

  Condition: Safari browser does not support data-list in HTML.

  Workaround: There is no workaround in Safari for this.

- CSCve00039

  Symptom: WAN interface shows status as down in IR800 after configuration using Quick Setup Wizard.

  Condition: WAN interface status is retrieved from show ip interface brief and other supported commands. The application lists the status as read from the device configuration. This issue is not consistently reproducible.

  Workaround: There is no workaround for this as application depends on IOS platform to provide the status.

- CSCvh67125

  Symptom: Enabling AVC is taking more than 45 seconds.

  Condition: The implementation is native to IOS. The following cli takes time to fetch data and it depends on the device response rate

  show ip nbar protocol-discovery [interface type number] [stats {byte-count | bit-rate | packet -count| max-bit-rate}] [protocol protocol-name | top-n number].

  Workaround: Launch AVC once and then the subsequent loadings should take less time.

- CSCvi41225

  Symptom: When no Sim is present in USB LTE, it does not show correct SIM status.

  Condition:
  USB LTE does not support the SIM status commands available for normal Cellular interfaces. The only way to fetch the sim status is via RSSI values. But the RSSI value does not change when SIM is removed. For details check the platform defect: CSCvf67829.

  Workaround: Do a modem-reset and wait for 3 to 5 minutes. Once modem is reset successfully, the modem details and the RSSI values are reflected correctly.

- CSCvi43525

Symptom: Access to monitor screens for build extracted in folder under root requires additional login.

Condition: IOS platform requires that the home htmls are placed directly under flash:. When this is not the case, the IOS design is such that it authenticates twice. This is platform design.

Workaround: Install CCP Express application under flash: or provide the authentication and save the credentials in browser.

- CSCvi45974

  Symptom: Occasionally getting error ?%NAT: Error deactivating CNBAR on the interface Cellular0/0? from the device while trying to remove ip nat from under the cellular interface.

  Condition: Issue happens randomly. Device gives error while trying to remove ip nat configuration. Applicable only on devices C841M-4X-JAIS/K9 and C841M-8X-JAIS/K9 when USB LTE modem is attached.

  Workaround: User will need to clear the unwanted configurations manually using CLI.

- CSCvi65481

  Symptom: Enabling AVC on IR device is not working.

  Condition: Enabling AVC throws error on configuring ip nbar http-services.The error thrown is "% NBAR Error: corrupted binary". This is because nbar 1 is not supported on IR devices.

  Workaround: There is no workaround for this as nbar1 is not supported on IR devices. The AVC feature will not be accessible on IR devices to prevent users from attempting configuration.

- CSCvi69904

  Symptom: Enabling IP Sec VPN is not working on IR Devices. Same is the case for Combination VPN for IPSecVPN+RemoteAccessVPN.

  Condition:On Hoover (IR829 M or B series) running IOS 15.7(3) or above, after enabling and configuring IP Sec VPN or the combination VPN of IPsec+RemoteAccess, no records are listed even though the configuration goes fine. This is because "show crypto session" is giving a blank output. This is a platform issue and is applicable for all IR 8x9 and 8x7 series devices.

  Workaround: The source interface for tunnel should have an IP address set. Without an IP address assigned, show crypto session gives blank output.

- CSCvm54225

  Symptom: Nano 4G modem hardware info is not shown.

  Condition: After issuing modem power cycle, the hardware info becomes "Hardware is Cellular, Modem not inserted". Due to this, the application cannot identify the same as LTE.

  Workaround: In some cases after user reloads the device, the hardware info is shown properly.

- CSCvj72539

  Symptom: CCP Express AVC feature does not work in IOS version 15.7(3)M2 and above.

  Condition: The 'ip nbar http-services' command is used to enable AVC and this throws the error "% NBAR Error: corrupted binary" when executed over http (via 'ios_web_exec/commandset'). In command line interface, this command works fine. Device Tested on is 841M, but could be applicable to all supported devices.

  Workaround: There is no workaround for this as the platform issue (CSCvj46796) needs to be fixed for the same. User has to use IOS version earlier to 15.7(3)M2 till a fix is rolled out in IOS for the same.

Resolved Defects

This following is the list of issues fixed in Cisco Configuration Professional Express Release 3.5.3:

- CSCvk58889

    Symptom: In MultiSite VPN, after configuring site is not appearing immediately.

    Condition: While creation of site, application checks for the new tunnels in a list. This list is not updated after the new tunnels are created. Since the tunnels are not present in the list, they are not listed.

    Workaround: User should navigate to any other screen and come back to VPN screen. The newly created site with the tunnel information will get loaded at this point

    Fix Details: As soon as the site is created, the same will get listed in the VPN screen with the details of the tunnel. This is done by refreshing the list of tunnels internally

- CSCvk21785

    Symptom: Alert for loading keeps on going when setting the L2L VPN through CCP. User is not able to configure sites in multisite VPN option.

    Condition: While creation of site, if remote subnets are not added, then application does not validate the same. Also, user might make the mistake of just entering the details in the input fields and forget to click on the "+" button which adds the entries to the remote subnet list. In these two cases, if user navigates through the VPN wizard by entering all other required details and clicks on Finish button, the VPN configuration is done without the remote subnets. Due to this, the output of "show crypto session" is rendered blank.

    Workaround: User should add the remote subnets when creating the site in multisite VPN.

    Fix Details: During creation of the site, if user does not enter the remote subnet details in the second tab of the VPN wizard and clicks on "Next" button, then user is not taken to the next step. Instead, the fields are highlighted in Red with the error message displayed on hover. If user had entered any valid values in the field before clicking on "Next", then post validation those would be added to the remote subnets list. This ensures that before the user clicks on "Finish" in the VPN configuration, the remote subnets are already in place.

- CSCvm10832

    Symptom: While removing dialer for Cellular Interface configured as backup WAN, both primary and backup interfaces in the WAN zone are removed.

    Condition: Gigabit Ethernet is primary WAN and Cellular Interface (with Dialer) is backup WAN. Security is enabled. Both GigE and Dialer2 are already in WAN Zone. User edits Cellular interface and changes option for Persistence to "No". After saving, the WAN zone gets cleared of all interfaces. This is incorrect as only the dialer for Cellular interface should get removed and the WAN zone should have both GigE and Cellular interfaces in it.

    Workaround: User has to move the earlier configured interfaces to WAN zone again.

    Fix Details: The application sets the Cellular interface as primary and sets the backup as none. Due to this, when the application does the cleanup as part of the configuration push, it removes all interfaces in the WAN Zone. This happens only when Cellular interface with persistence is set as backup. The fix addresses to read the Primary and Backup interfaces correctly in all scenarios so that the removal of the right interface (dialer for Cellular) from and adding back the Cellular interface to WAN zone is in effect.

- CSCvm38968

Symptom: User edits Cellular interface and sets the data and attach profiles. User is shown an error message that there is an error trying to fetch the profile info and user should try after sometime.

Condition: When editing profile info for the first time on a router via advanced configuration under Interfaces section, an error is shown "Error occurred while fetching interface data. Please retry after sometime.".

Workaround: User has to consider this as a warning message and go ahead and create the profiles as required..

Fix Details: The error message is updated to advice the user to proceed when profile is not found..

- CSCvm10668

Symptom: User loads Cellular interface and sees details wrong. When edit operation is performed, configuration issues/errors may be noticed.

Condition: User tries to edit Cellular interface right after Day0 configuration. The existing config is not loaded properly. So edit operation on Cellular interface right after Day0 configuration leads to configuration issues and errors. This can happen in Advanced configuration too, when modem power cycle is initiated.

Workaround: User has to wait for minimum of 5-10 minutes for the Cellular interface and modem to be back up after the power cycle issued on the modem during the day 0 configuration. User has to reload the page so that the latest details on the interface is fetched.

Fix Details: Edit and delete options on the interface is hidden and a warning icon is displayed against the Cellular interface in the Interfaces table. Upon hovering on the warning icon, the user is informed that the interface data could not be loaded and user is suggested to retry after sometime. To enable the user to do this from the same page, a "Refresh" button has been added to the top of the page.

Related Documentation

Additional documentation available for the Cisco Configuration Professional Express are:

- Cisco Configuration Professional Express Feature Guide
- Cisco Configuration Professional Express Quickstart Guide
- Cisco Configuration Professional Express Administration Guide