Firmware Version: 4.4.1.2_WW
4.4.1.2_RU

Published Date: 2015-08-03

Copyright © 2015

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Content:

dlink green

Revision History and System Requirement:

Firmware Version	Date	Model Hardware	History
4.4.1.2_WW 4.4.1.2_RU	03 Aug 2015	DWC-1000 A1/B1	1. New GUI firmware 2. On top of FW v4.4.1.1 3. Bug fix
4.4.1.1_WW 4.4.1.1_RU	22 May 2015	DWC-1000 A1/B1	1. New GUI firmware 2. On top of FW v4.4.0.2_B501
4.4.0.2_B301_WW 4.4.0.2_B301_RU	13 Mar 2015	DWC-1000 A1/B1	1. Bug fix
4.4.0.2 4.4.0.2	02 Mar 2015	DWC-1000 A1/B1	1. Bug fix
4.3.0.2_B401_WW 4.3.0.2_B401_RU	03 Dec 2014	DWC-1000 A1/B1	1. Bug fix
4.3.0.2_B305_WW 4.3.0.2_B305_RU	25 Nov 2014	DWC-1000 A1/B1	1. Bug fix 2. Security Vulnerability Addressed OpenSSL vulnerability (CVE-2014-3566)
4.3.0.2_B203_WW 4.3.0.2_B203_RU	05 Nov 2014	DWC-1000 A1/B1	1. DWC-1000 and DWC-2000 are **not** vulnerable to SRTP Memory Leak (CVE-2014-3513).
4.3.0.2_B101_WW 4.3.0.2_B101_RU	11 Sept 2014	DWC-1000 A1/B1	N/A
4.3.0.2_WW 4.3.0.2_RU	12 Aug 2014	DWC-1000 A1/B1	1. Security Vulnerability Addressed OpenSSL vulnerability (CVE-2014-0224)
4.3.0.1_WW 4.3.0.1_RU	17 July 2014	DWC-1000 A1/B1	1. New AP support 2. Bug fix 3. Based on 4.2.0.6_B501
4.2.0.6_WW_B303 4.2.0.6_RU_B303	11 Apr 2014	DWC-1000 A1	1. DUSA20140204000002 2. Security Vulnerability Addressed
4.2.0.6_WW_B201 4.2.0.6_RU_B201	11 Mar 2014	DWC-1000 A1/B1	1. Bug fix 2. Security Vulnerability Addressed
4.2.0.6_WW 4.2.0.6_RU	03 Mar 2014	DWC-1000 A1/B1	1. Add firmware MD5 checksum info 2. Update "Important Notes" 3. Update "Notes for Configuration Auto-Backup/Restore in USB Storage"
4.2.0.6_WW 4.2.0.6_RU	30 Dec 2013	DWC-1000 A1/B1	1. Security Vulnerability Addressed
4.2.0.3_WW 4.2.0.3_RU	27 June 2013	DWC-1000 A1	1. Update Known Issue
4.2.0.3_WW 4.2.0.3_RU	1 Apr 2013	DWC-1000 A1	1. Security Vulnerability Addressed
4.1.0.2_10222W 4.1.0.2_10222R	22 May 2012	DWC-1000 A1	
4.1.0.2_10204W 4.1.0.2_10204R	1 Feb 2012	DWC-1000 A1	

1.01B67_WW 1.01B67_RU	26 Dec 2011	DWC-1000 A1	

Firmware Details:

Image Version	HW	MD5 Checksum
DWC-1000_A1_FW_4.4.1.2_WW	A1	8f3d6b41dc3a10d01252997350a0db65
DWC-1000_A1_FW_4.4.1.2_RU	A1	e274f1fffcaf70226cfb9d726732fa1d
DWC-1000_B1_FW_4.4.1.2_WW	B1	5a001e3db21feeb178e2cbf77d1b292c
DWC-1000_B1_FW_4.4.1.2_RU	B1	f3ce46103c53fe90fce362fc2dfbeaf2

Important Notes:

1. A firmware region mismatch between RU and WW images now is forbidden. System will check and block firmware upgrade process, such as firmware upgrade from RU→WW or WW→RU image.

2. Below are new functions and will be available after upgrading FW to v4.2.0.3 or later.

Website Filter feature (Content Filtering/ Approved URLs/ Blocked Keywords/ Export) needs DWC-1000-VPN/ DWC-1000-VPN-LIC license upgrade.

Category Filtering feature needs DWC-1000-WCF-12 or DWC-1000-WCF-12-LIC license upgrade.

3. B1 firmware is not backward compatible with HW A1, please make sure the hardware version is correct before upgrading firmware for DWC-1000.

4. Hardware B1 supports **Web Recovery Mode** whenever there is firmware damage on DWC-1000, or manually access it by following steps: Power off the DWC-1000, press and hold the reset button, then power on and keep hold the reset button for over 15 seconds, the DWC-1000 will enter the Web Recovery Mode either.

The IP address will be 192.168.1.1, and make sure to setup same IP segment for your PC/NB then access the Web Recovery Mode via browser.

5. GNU/Linux Bash Shell vulnerability (CVE-2014-6271)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since these devices do not expose the shell interface through CLI nor WEB interface (including CGI).

Reference website:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

http://seclists.org/oss-sec/2014/q3/650

https://blogs.akamai.com/2014/09/environment-bashing.html

6. SRTP Memory Leak (CVE-2014-3513)

We have evaluated this vulnerability. DWC-1000 and DWC-2000 are **not** vulnerable to this since

these devices do not support SRTP and based on OpenSSL 1.0.x versions.

Reference website:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3513

Notes for Configuration Auto-Backup/Restore in USB Storage:

D-Link DWC Unified Controller support configuration backup or restore automatically while a USB drive is inserted. Following information instructs what condition will perform backup/restore.

1. The configuration will be automatically backed up to the USB drive as soon as the USB drive is inserted. The configuration file name format is <Model Name>_<Serial Number>.cfg.
2. The system LED on the DWC blinks 5X in amber to indicate a backup operation has started.
3. The configuration in the USB drive can be updated if the user manually clicks 'Save Settings' in any GUI page and provided the Model Number and the Serial Number of the DWC matches with the file already present in the USB drive.
4. In case of reboot, the DWC checks for the presence of configuration file (with format ModelName_SerialNumber.cfg). If found, the configuration from the USB drive is restored on the DWC. If a configuration file with the correct format is present in both connected USB drives, the configuration from the first USB drive will be used to restore the DWC.
5. The USB drive can have only one configuration with the above mentioned format for each model name.
6. If the USB drive is plugged in to the DWC which is in factory default state, then during reboot, no backup is taken since no custom configuration file exists in the DWC by that time. The custom configuration is stored on the USB drive once the user clicks Save Settings in any GUI page.

Upgrading Instructions:

Upgrading by using Web-UI

For installation details and upgrade instructions, please refer to the Firmware Upgrades chapter in the *DWC-1000 User Manual ver. 1.01.*

New Features:

Firmware Version	New Features
4.4.1.2_WW 4.4.1.2_RU	N/A
4.4.1.1_WW 4.4.1.1_RU	1. DWL-6610AP support (DWL-6610_FW_v_4.3.0.2_B042.tar or later version)

	2. WDS-managed AP feature for 6610AP is not ready yet 3. [HQ20141204000016] WLAN visualization issues--**Not** supported for A1 hardware for new GUI image, but B1 supported.
4.4.0.2_B301_WW 4.4.0.2_B301_RU	N/A
4.4.0.2_WW 4.4.0.2_RU	1. Maximum Clients 30 as default 2. Update Russia Time Zone 3. DWL-6700AP support (DWL-6700_FW_v4_4_0_6.bin or later version)
4.3.0.2_B401_WW 4.3.0.2_B401_RU	N/A
4.3.0.2_B101_WW 4.3.0.2_B101_RU	1. Increase the DHCP IP leasing scope (/22, 255.255.252.0) Example: WEB GUI **LAN IP Address Setup** IP Address: 192.168.8.1 Subnet Mask: 255.255.252.0 List of Available DHCP Pools | Start IP Address	End IP Addresss | |---|---| | 192.168.8.2 | 192.168.8.254 | | 192.168.9.2 | 192.168.9.254 | | 192.168.10.2 | 192.168.10.254 | | 192.168.11.2 | 192.168.11.254 | Edit Delete Add Example: Setting LAN IP and DHCP server via CLI command ** D-Link DWC> net lan ipv4 configure net-config[lan-ipv4]> static address 192.168.8.1 net-config[lan-ipv4]> static subnet_mask 255.255.252.0 net-config[lan-ipv4]> save net-config[lan-ipv4]> .top D-Link DWC> D-Link DWC> net dhcp-pool-config add net-config[pool-config]> vlanid 1 net-config[pool-config]> start_address 192.168.8.2 net-config[pool-config]> end_address 192.168.8.254 net-config[pool-config]> save net-config[pool-config]> vlanid 1 net-config[pool-config]> start_address 192.168.9.2

```
net-config[pool-config]> end_address 192.168.9.254

net-config[pool-config]> save

net-config[pool-config]> vlanid 1

net-config[pool-config]> start_address 192.168.10.2

net-config[pool-config]> end_address 192.168.10.254

net-config[pool-config]> save

net-config[pool-config]> vlanid 1

net-config[pool-config]> start_address 192.168.11.2

net-config[pool-config]> end_address 192.168.11.254

net-config[pool-config]> save

net-config[pool-config]> .top

D-Link DWC>

D-Link DWC> net lan ipv4 configure

net-config[lan-ipv4]> dhcp mode DHCP-Server

net-config[lan-ipv4]> dhcp default_gw 192.168.8.1

net-config[lan-ipv4]> save

net-config[lan-ipv4]> .top

D-Link DWC>
************************************************
```

2. Reboot Scheduler via CLI command

```
************************************************
D-Link DWC> util schedule-reboot true

Operation Succeeded

…

D-Link DWC> Reboot Reason : reboot scheduler

The system is going down NOW !!

Sending SIGTERM to all processes.
************************************************
```

a. Enable: "util schedule-reboot true"

b. Disable: "util schedule-reboot false"

c. It will reboot every day automatically during 03:01:10 – 03:01:50, not 3AM sharp.

3. Reboot Trace Code via CLI command

```
************************************************
D-Link DWC> show system status

System Info
```

_____

System Up Time: 0 days, 0 hours, 2 minutes, 49 seconds

Reboot Trace Code: reboot scheduler

ModelId: DWC-1000

System Name: DWC-1000

WLAN Module Version: 4.2.0.1

Firmware Version: 4.3.0.2_A1_B101_WW

Serial Number: QBE81B6000004

UBOOT_VERSION: N/A

****

4. Deleting local user via CLI command

****

D-Link DWC> system group add

groups-config[userdb]> groupname CP

groups-config[userdb]> description Captive-Portal

groups-config[userdb]> Privilege_Type CaptivePortal Y

groups-config[userdb]> grouptimeOut 10

groups-config[userdb]> save

groups-config[userdb]> .top

D-Link DWC>

D-Link DWC> system users add

users-config[userdb]> username fatman

users-config[userdb]> password 12345678

users-config[userdb]> password_confirm 12345678

users-config[userdb]> groupname CP

users-config[userdb]> FirstName Fatman

users-config[userdb]> LastName Chen

users-config[userdb]> save

users-config[userdb]> .top

D-Link DWC> show system users all

-------------USERS----------------

_____

 ROWID User Name Group Login Status

_____ _____ _____ _____

 1   admin   ADMIN Enabled (LAN) Enabled (OPTION)

 2   guest   GUEST Disabled (LAN) Disabled (OPTION)

	3 fatman CP Enabled (LAN) Enabled (OPTION) D-Link DWC> system users delete_user fatman STATUS_OK D-Link DWC> show system users all -------------USERS---------------- _____ ROWID User Name Group Login Status _____ _____ _____ _____ 1 admin ADMIN Enabled (LAN) Enabled (OPTION) 2 guest GUEST Disabled (LAN) Disabled (OPTION) D-Link DWC> ** a. Delete via User Name: "system users delete_user fatman" b. Delete via ROW ID "system users delete 3"
4.3.0.2_WW 4.3.0.2_RU	N/A
4.3.0.1_WW 4.3.0.1_RU	1. DWL-8610AP Support (DWL-8610_FW_v_4.3.0.2_B016) 2. Delete/deactivate licenses via CLI command ** D-Link DWC> license clear ** 3. The Max AP database number is 4 times of Max Managed AP number supported on DWC-1000. {{TABLE}}
4.2.0.6_B303_WW 4.2.0.6_B303_RU	N/A
4.2.0.6_B201_WW 4.2.0.6_B201_RU	N/A
4.2.0.6_WW 4.2.0.6_RU	N/A
4.2.0.3_WW 4.2.0.3_RU	1. Captive Portal enhancements 2. WCF with License support 3. WLAN Wizard enhancements 4. VPN Failover support 5. DWL-2600AP support 6. WLAN Visualization enhancements

Table embedded in row 4.3.0.1:

AP license	Default	AP6 x 1	AP6 x 2	AP6 x 3
Max AP database	24	48	72	96
Max Managed AP	6	12	18	24

	7. Additional Authentication Mechanisms 8. Hotspot support 9. WDS support
4.1.0.2_10222W 4.1.0.2_10222R	1. Add Auto Refresh check box on AP monitoring pages. 2. In Valid AP page Radio section Automatic power drop down section 0 should be replaced by Profile
4.1.0.2_10204W 4.1.0.2_10204R	1. Integrated WLAN module v 4.1.0.2 2. Compatible with DWL-8600AP, DWL-6600AP and DWL-3600AP firmware v 4.1.0.x. 3. Compatible with DWL-8600AP firmware v 3.x.x.x for AP discovery and firmware upgrade 4. Advanced VLAN, includes MAC VLAN, Protocol VLAN, Voice VLAN, Double VLAN, and GVRP 5. Advanced QoS, includes Policy-based LAN QoS, Port Shaping Rate, Flow Control, and Auto VoIP 6. Customized captive portal page on WLAN Captive Portal 7. MIB support (Firmware Upgrade, Configuration Backup, Configuration restore and system properties) 8. RADIUS server integration for PAP and CHAP
1.01B67_WW 1.01B67_RU	This version compatible with DWL-8600AP firmware v4.1.x.x.

Problems Fixed:

Firmware Version	Problems Fixed
	1. 51638 P1 DBG14090381 Unable to see the fields e.g. Header, Customized Not, Time Stamp and Footer. 2. 51641 P1 DBG14090416 incorrect CP type in AP Profile SSID page. 3. 51642 P1 DBG15050481 Reboot message incorrect 4. 51647 P1 DBG15050404 DWL-2600 & 8610AP not support WEP encryption, so DWC-1000 should not have the option. 5. 51648 P1 DBG15050482 Cannot find select all button 6. 51712 P2 DBG15050472 For managed AP,5G and 2.4G display should reverse in "RF scan" page for 8610 AP 7. 51713 P2 DBG15050478 unable to set more than 16 characters in the user name for PPPOE setting when using Wizard to setup PPPOE. 8. 51714 P2 DBG15050477 Can't type "@" and "." when we choose PPPoE

	connection type in "internet connection wizard".
	9. 51715 P1 DBG15050485 display incorrect info on Managed AP page
	10. 51716 P1 DBG15050489 Wireless switch task dead
	11. 51778 P2 DBG12050169 DWC WEB GUI logout after some time operation(randonly), need to login again to use.
	12. 51780 P2 DBG15050416 firmware download behavior in DWC-1k must be changed
	13. 51781 P2 DBG13120227 Managed AP status radio details must be properly displayed for 8610 AP
	14. 51782 P1 DBG13120226 The 5Ghz radio shall display 802.11a/n/ac supported in Default profile.
	15. 51269 P2 Ap profile radio mode page description is showing wrong for Radio 1 and Radio 2 operate modes
	16. 51842 P2 Unable to change Country code to BR
	17. 51846 P2 Captive Portal redirect feature does not works on mobile device
	18. 51852 P2 LAN leased clients entries are flushed if we add new VLAN in the device in DWC1000
	19. 51853 P2 Syslog: Client Association/Roaming/Disassociation logs not showing the location information
	20. 51854 P2 Channel information is incorrect on Managed AP page in DWC1000
	21. 51855 P2 Tablet(or IPAD) and cell phone does not display correct captive portal page in DWC1000
	22. 51856 P2 Issues with WLAN visualization page in DWC-1000
	23. 51863 P2 Unable to configure the limits for bandwidth in option qos page
	24. 51873 P2 Support for SNMP QoS Differentiated Services in DWC-1000
	25. 51874 P1 Need to add more IP address(1024) list at the L3 discover page for DWC-1000
	26. 51875 P1 Unable to obtain all OIDs in MIB browser on performing walk operation
4.4.1.1 4.4.1.1	1. 49916 P1 Observed critical error after STA pass captive portal Login in IE11 browser(DWC-1000)
	2. 50003 P1 DHCP server in vlan is not responding when configured relay on another vlan (4.4.0.2_B401)
	3. 50169 P1 Unable to upgrade firmware to 8610-AP from DWC-1000 (4.4.0.2_B401)
	4. 50333 P1 Unable to see the channel suggestion for 5 ghz (4.4.0.2_B402)
	5. 50356 P1 Need to add DWL-6610 AP support in DWC-1000 device

	(4.4.0.2_B401) 6. 50392 P1 Unable to push the radius server details to DWL-6600 AP from DWC-1000 device (4.4.0.2_B401) 7. 50524 P1 The DWL-6700 did not support WEP encryption (4.4.0.2_B402) 8. 50596 P1 Hardware Name is wrong for DWL-8610 ap in DWC-1000 device (4.4.0.2_B501) 9. 51080 P1 Need to apply changes for vulnerability CVE-2015-0291 / CVE-2015-0204. (4.4.0.2_B501) 10. 51258 P1 Java applet should load with latest java versions in B1 Hardware 11. 51263 P1 Wlan visualization should work similar to 4.3.0.1 image for A1 hardware 12. 51331 P1 HQ20141104000020 Not able to perform trace route or ping functionality of ipV6 addresses from diagnostics page 13. 51344 P1 HQ20150119000014 Radio mode is saving as 802.11b/g in AP Profile Radio page when we save it as 802.11b 14. 51348 P1 HQ20141128000005 Observed Status of Physical mode in RF scan page is not showing properly in DWC-1000 using DWL-8610AP
4.4.0.2_B501_WW 4.4.0.2_B501_RU	1. 50596 P1　　HQ20150401000014　　The HW type naming issue of DWL-8610AP 2. 47777 P1　　HQ20140804000014　　Intermediate Restart[DRU20140730000001-Middle East] 3. 51080 P1　　N/A Open SSL Vulnerability patches
4.4.0.2_B402_WW 4.4.0.2_B402_RU	1. 50333 P1 DBG15030267 Auto-channel function not work in the DWC-1000 with the fixed time setting 3. 50333 P1 HQ20150127000021 Auto Channel in 5G not work properly [DUSA20150122000002-USA] 4. 50524 P1 DBG15030277 The DWL-6700 did not support WEP encryption, but controller has the option
4.4.0.2_B401_WW 4.4.0.2_B401_RU	1. 50169　　P1　HQ20150305000004　　DWC-1000 - error by updating APs[DEUR20150304000004-Central Europe] 2. 50003　　P1　HQ20141209000011　　SHCP server stopped working[DEUR20141021000006-Eastern Europe] 3. 50356　　P1　N/A Need to add DWL-6610 AP support in DWC-1000 device 4. 50392　　P1　N/A Unable to push the radius server details to DWL-6600 AP from DWC-1000 device
4.4.0.2_B301_WW 4.4.0.2_B301_RU	1. [DUSA20141119000004][HQ20141121000004] Display error of Controller

	MAC Address on AP Details
	2. [DEUR20150130000005][HQ20150202000005] DWC-1000 - scheduler
	3. [DI20150211000005][HQ20150212000006] DHCP server for each VLAN
	4. [HQ20150210000018] Incorrect usage-left info shown in the log-out web page
	5. Trap Log Enhancement. To sync the Log behavior from DWS-4026 for DJP
	SPEC: SNR-20141118-001/ ACA diff_91 (auto channel algorithm)
	DWS-4026 DTrack case: DEUR20140918000007/HQ20140919000018
	FW: DWS-4026_4.3.0.3_B016
4.4.0.2 4.4.0.2	N/A
4.3.0.2_B401_WW 4.3.0.2_B401_RU	1. [DLA20140829000002][HQ20140829000007] Problem with vlan 2. [DEUR20141024000002][HQ20141027000007] DWC-1000 - becomes unresponsible 3. DBG14080374
4.3.0.2_B305_WW 4.3.0.2_B305_RU	1. [DEUR20140912000008][HQ20140915000017] DWC-1000 VPN LIC - Auto-Rollover OPT 1 - 2 DDNS not updated 2. OpenSSL vulnerability (CVE-2014-3566) Security Vulnerabilities Addressed: OpenSSL before 0.9.8za, which allows man-in-the-middle attack, and consequently hijack sessions or obtain sensitive information. Reference: CVE-2014-3566 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566 Solution: For the fix for this vulnerability issue, we did not upgrade OpenSSL. Rather we selectively merged the required changes to resolve the issue into the current OpenSSL version 0.9.8za. 3. [DEUR20141110000005][HQ20141111000010] DWC-1000 & DWL-8610 - no 80 MHz choosable for country CH
4.3.0.2_B101_WW 4.3.0.2_B101_RU	1. [DEUR20140722000001][HQ20140724000011] DWC-1000 - expiration time in Frontdesk 2. [DEUR20140722000002][HQ20140729000005] automatic reboot (Schedule Reboot) 5. [DEUR20140605000008][HQ20140624000021] Temp CP Expiration Issue (not gateway, it failed when using the config file from OBU, SPR#46076)
4.3.0.2_WW 4.3.0.2_RU	1. OpenSSL CCS Injection vulnerability (man-in-the-middle attack) **Security Vulnerabilities Addressed:** OpenSSL before 0.9.8za, which allows man-in-the-middle attack, and consequently hijack sessions or obtain

sensitive information.

Reference: CVE-2014-0224

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224

https://www.openssl.org/news/secadv_20140605.txt

Solution: Update OpenSSL patch to 0.9.8za that addresses the vulnerability.

2. Sync DWS-4026 Auto Channel Algorithm Patch at 5GHz Issue (DI20140507000005)

3. JAVA update for wireless controller

4. [DEUR20140603000004][HQ20140604000004] DWC-1000 & DWL-2600AP - issue with WPA key after DWC-reboot

5. [DEUR20140522000001][HQ20140523000004] DWC-1000 - CP time doesn't count down in browser after logging

   a. [44444] Usage time will get count down automatically without clicking the "F5" button or refresh button. (Resolved in v4302)

   b. In **View Accounts** page of FrontDesk, after pressing the "F5" or refresh button in IE11 browser, the FrontDesk user is re-directing to login page (get logged out). (v4302 didn't include this IE11 support enhancement)

6. [DEUR20140106000001][HQ20140218000024] DWC-1000 - maximum detected client limit too low

7. [DEUR20140605000008][HQ20140624000021] DWC-1000 - time CP - expired used won't be deleted (Temporary user cannot login CP page when the daylight saving was enabled)

4.3.0.1_WW 4.3.0.1_RU	1. [DEUR20140131000006][HQ20140205000020] CLI error while configuring SSID. 2. [DEUR20140305000004][HQ20140306000015] DWC-1000 VPN LIC - issue with upload at german eMail provider (gmx.de/gmx.net) 3. [DRU20140430000002][HQ20140507000013] Problem with the Epson

	1945W projector (Issue resolved: Cannot upgrade firmware for 2600AP via DWC-1000) 4. Memory leak issue (Spontaneously reboot every 2.5 - 3 hours, or sometimes reboot randomly)

4.2.0.6_B303_WW
4.2.0.6_B303_RU
	1. [DUSA20140204000002][HQ20140219000015] Unacceptable Download Speeds Using the DWL-2600AP Controlled by the DWC-1000.
	2. **Security Vulnerabilities Addressed:** Null byte injection attack in URL.
	  Reference: http://www.ultsec.com/null-byte-attack.php
	  Solution: Avoid parsing the null byte in URL and send back that requested URL is not there.

4.2.0.6_B201_WW
4.2.0.6_B201_RU
	1. [DEUR20140117000008][HQ20140120000016] DWC-1000 - password issue.
	  Security Vulnerabilities Addressed: Using the character "$" in the login password causes the password to get truncated to only the characters prior to it, potentially shortening and simplifying the original password. This only affects the CLI login, Web login is not affected and can accept the "$" character in the password login.
	  Reference: N/A
	  Solution: Fixed CLI login to recognize the "$" character properly.
	2. [DI20130821000001][HQ20130823000011] Cannot configure RADIUS Accounting.
	3. [DRU20140116000005][HQ20140114000010] Fail to use 5G channel on country code in Russia.
	4. [DEUR20140131000006][HQ20140205000020] CLI error while configuring SSID.

4.2.0.6_WW
4.2.0.6_RU
	1. [DI20130404000005][HQ20130408000025] CLI issue and request.
	2. [DI20130405000001][HQ20130408000014] RADIUS Use Network Configuration cannot be disabled in CLI.
	3. [DI20130327000006][HQ20130328000003] The maximum number of AP can be registered into local valid DB.
	4. [DI20130108000020][HQ20130109000007] Internet Throughput (PPPoE).
	5. [DEUR20130426000003][HQ20130426000017] SNAT Issue.
	6. HTTP 500 Error
	  a. [DRU20130708000006][HQ20130709000013]
	  b. [DEUR20130708000003][HQ20130730000015]
	  c. [DI1208120001]

7. [DEUR20130410000003][HQ20130411000011] captive portal, billing.

8. [DEUR20130412000004][HQ20130424000016] DWC-1000 LDAP, DSR-1000N PPTP.

9. LDAP Issue

  a. [DEUR20130412000004][HQ20130424000016] DWC-1000 LDAP, DSR-1000N PPTP

  b. [DEUR20130528000001][HQ20130530000017] DWC-1000 - CP with AD LDAP integration

  c. [DEUR20130523000012][HQ20130530000014] LDAP doesn't work

10. [38483][DEUR20130531000007][HQ20130603000006] DWC-1000 -NT-Domain & AD integration.

11. [DI20130329000002][HQ20130401000007] Do not support 802.11an or 802.11bgn for country code KR.

12. [DEUR20130507000003][HQ20130510000004] create corrupted config file – doesn't save config.

13. [DI1208120001] SNMP Trap Enhancement (P-Force/Ilya Narodetsky).

14. [DI20130404000001][HQ20130408000013] Warning displays by command to add RADIUS.

15. [DI1208120001][HQ20130508000011] No Response on SNMP Query issue, workaround is to configure "Syscontact" and "SysLocation" fields and DWC-1000 will start passing SNMP query. (P-Force/Ilya Narodetsky).

16. [DRU20130620000005][HQ20130621000011] WDS Status & notifications.

17. [DEUR20130621000009][HQ20130624000009] Hotspot mode kernel panic.

   Maximum Local Database Users: 400

   Maximum Billing Profile Users: 256

18. [HQ201307020000010] Continuous case for DWC LDAP server checks issue.

19. [DEUR20130621000007][HQ20130624000005] DWC1000 - remote logging via eMail.

20. [DEUR20130722000010][HQ20130802000002] WLAN Visualization doesn't work.

21. Browser issue

  a. [DEUR20130523000001][HQ20130409000009] AP profile applying with IE10 and Chrome.

  b. [DI20130409000001][HQ20130409000009] Peer Controller Configuration Request does not start.

22. Temporary Account Enhancement

    a. [DEUR20130410000003][HQ20130411000011] captive portal, billing (an existing ticket cannot be deleted)

    b. [DEUR20130611000003] DWC-1000 – How to delete CP temporary user

    c. [DEUR20130424000010][HQ20130425000002] DWC-1000 - CP with Ticketing - How to log CP users?

23. [HQ20130812000006] billing account users are not getting expired.

24. [DEUR20130715000001][HQ20130715000008] DWC-1000 - CP with POP3 auth not working.

25. [HQ20130708000010] The DWC Generated the wrong number of billing users account.

26. [DI20130716000001][HQ20130716000019] Full tunnel failed on DWC with DSR..

27. [DEUR20130613000007][HQ20130805000004] DWC-1000 - CP issue with guest users.

28. [DUSA20130608000002][HQ20130621000018] Captive Portal (Page does not refresh and redirect).

29. [DEUR20130430000005][HQ20130502000010] Customized CP doesn't work with mobile devices.

30. [DEUR20130708000003][HQ20130730000015] DWC-1000 - Cluster problems.

31. [DRU20130718000003][HQ20130723000010] DWC-1000: DHCP relay issue.

32. [DEUR20130912000005][HQ20130913000006] multiple subnets show.

33. [DEUR20130213000002][HQ20130218000031] DWC-1000 & ALL APs - several issues with Peering.

34. Vulnerability reported by DEU (nu11.nu11@yahoo.com 2013-08-18) Network access to the router ports 443 and 23.

    Security Vulnerabilities Addressed: Devices respond clients some unnecessary information, and hence give hackers a chance to get a non-persistent root shell.

    Reference: CVE-2013-5945, CVE-2013-5946

    http://packetstormsecurity.com/files/124319/D-Link-DSR-Router-Remote-Root-Shell-Overview.html

    http://dl.packetstormsecurity.net/1312-advisories/dlinkdsrrouter-writeup.txt

    http://web.nvd.nist.gov/view/vuln/search-results?query=Dlink&search_type=all&cves=on

	Solution: Remove all unnecessary root user account
	35. [DEUR20130906000003][HQ20130909000005] DWC-1000 - PPTP Routing similar to case DEUR20120814000019
	36. [HQ20131001000009] "show system dashboard" command in CLI is not showing up with any value, until we go the status general page in GUI
	37. [DRU20130620000009][HQ20130621000008] DWC-1000: Country code and 802.11n issue
	38. [DI20130902000002][HQ20131204000011] Created time of temporary user is showing GMT time only after changing GMT + local time also
4.2.0.3_WW 4.2.0.3_RU	1. [DEUR20121030000003][HQ20121016000005] Device management
	2. Not able to upload .csv file into the device in DWC-1000
	3. [HQ20130218000043] click enter in system check page will auto logout
	4. [DEUR20121126000009][HQ20121127000016] VLAN problem (L2 VLAN discovery)
	5. [HQ20121023000015] name and password in Captive portal login page are changing to unreadable format
	6. [DEUR20121206000011][HQ20121210000014] 'Change password' option when user log in over CP
	7. [DEUR20130122000009][HQ20130124000014] SSID CaptivePortal is not working in L3 Network Setup
	8. Fix CP Profile Usage Status display. Enabled and Disabled.
	9. After enabling the DHCP server from CLI if we try to re enable it from GUI device is not allowing to enable LAN DHCP-Server without configuring WINS server.
	10. Kernel panic DHQ reported.
	11. Wireless security parameters for WPA/WPA2 are showing wrong in SSID page.
	12. Idle timeout and session timeout for captive portal users is not working with custom SSID after reboot.
	13. UPnP vulnerabilities reported by DJP.
	14. [HQ20130110000001] Device is not re-directing to particular captive portal page configured for a SSID from wireless client.
	15. [HQ20130104000010] In IE9(64 bit) Authentication server options are greyed out in Captive portal SSID setup page.
	16. CLI command didn't show all info. (UDP Connection limit/ Allow Ping from LAN).
	17. [HQ20130130000029] Need to change the file name of 'teamf1.cfg.ascii' file to 'dwc.cfg.ascii' in DWC configuration.

18. [DBG13020040][DBG13020037] Need to add a red warning message in category filtering settings while enabling category filtering to mention content filtering settings will be impacted when category filtering is enabled.

19. [DLA20120816000003][HQ20130104000007] Captive Portal profile settings are not reflecting in IE9 (64 bit). (CP customization does not work on all browsers)

20. [DGC20121129000001][HQ20121128000012]   Cannot delete users after upgrading from 4.1.0.2-10222 to 4.1.0.2-10261W.

21. [DGC20121101000003][HQ20121102000001] Need support for Logs when user login to the captive portal.

22. [DEUR20120816000013] Remote management port 443 issue, changing the default setting to port 4443.

23. [DLA20120811000002][HQ20120814000010] Disable "Block TCP flood" by default setting.

24. [HQ20130104000009] Admin user session is timed out when after clicking on preview button in captive portal setup page in I.E browser.

25. [HQ20120924000006] Can we telnet to the DSR, DWC through WAN

26. [DLA20120912000002][HQ20120912000003] How to create a configuration script

27. [DEUR20121128000007][HQ20121129000015] Backdoor/security issue. (nu11.nu11@yahoo.com 2012-11-25)

    Security Vulnerabilities Addressed: Persistent root access.

    Reference:

    http://packetstormsecurity.com/files/118355/D-Link-DSR-250N-Backdoor.html

    Solution: Removed CLI commands that could allow someone to overwrite the super user password and gain root access to the device. Root user

28. account will be completely removed in the next firmware version. [DEUR20120709000008][HQ20120710000014] Can't configure global action in client authentication

29. [DLA20120816000003][HQ20120817000016] High Customized Captive Portal

30. [HQ20120921000002] Urgent DWC break down after the user try to authenticate with the RADIUS server.

31. [DGC20120907000004][HQ20120911000002] Device is redirecting to captive portal logout page while trying to access internet.

32. [DEUR20120724000007][HQ20120725000006] Check box for selecting

	SSID's in AP profile--Configure SSID's page are greyed out when the hardware type for AP profile is selected as DWL-3600.
	33. [DEUR20120710000006][HQ20120711000010] Unable to configure WPA/WPA2 key with special characters from Advanced --> SSID page.
	34. [HQ20120928000003] Device is displaying '500 internal server error' while trying to login to captive portal with radius authentication when radius server contains additional info for user in users file.
	35. [HQ20121009000003] While device is rebooting able to see weird logs in the device shell.
4.1.0.2_10222 W 4.1.0.2_10222 R	1. AP L2 VLAN discovery is not support.
	2. Unable to establish tunnel in L2 distributed Tunneling Mode.
	3. While getting the firmware version using the mib browser region code is missing.
	4. Device is not showing Firmware version with region in CLI.
	5. GUI is displaying firmware version without WW in SSL VPN client page after login.
	6. Sometimes a pop-up window shows up with Captive Portal Login page
	7. In Advanced page, wording is abnormal. It shows options like 'Submit' and 'Don't Save Settings', instead 'Submit' and 'Don't Submit Settings'.
	8. GUI look and feel is not good in "poll list", "local oui database" and in Edit Channel/Power of manual management pages.
	9. Clicking on the traffic dashboard page, the very first time after a power-cycle of the box, may result in an internal error page.
	10. Traffic not following flow based QoS policy for default services and custom service added with type "BOTH".
	11. Clustering support for customized captive portal is not supported.
	12. Captive Portal disconnect management is not working.
	13. System log is not working
	14. [DBG11110021] In CLI in the warning message 'The de-authentication attack is disabled' the character "T" is missing.
	15. [DBG11110301] The captive portal created profiles are not listed on captive portal interface association page
	16. [DBG11110305] After disconnecting the captive portal session manually from the GUI of the device still able to run the traffic from wlan host without further authentication
	17. [DBG11110308] There should be one verification mode for captive Portal for lan side and wlan side
	18. [DBG11110309] The defined captive portal profiles cannot be applied on

	WLAN interface.
	19. [DBG11120016]SAVE SETTINGS button is shown as SUBMIT in SNMP Trap and Distributed tunneling pages.
	20. [DBG11110094] The descriptions for distributed tunneling page to be updated.
	21. [DBG11110092] There is no description on WAN CP Interface Association page.
	22. [DBG11110029] AP Hardware Capability List only shows DWL-8600AP on WEB, but CLI can shows all 8600AP, 3600AP and 6600AP.
	23. [DBG12020124] "Dhcp" word must be displayed in capital letters in lan dhcp leased clients page
	24. [DEUR20120402000003][DUSA20120321000002] SSID setup page has critical text errors on WPA and WPA2. It is also mapping to D-track case
	25. [DEUR20120402000003] Access the page of All AP Status without authentication.
	26. Help content need to be updated available for some WLAN pages.
	27. External Authentication support in wired captive portal is not available.
	28. <Spec Update> IPv6 address AP discovery/ management/ monitoring are not support.
	29. <Spec Update> L3 tunnel (IP-IP tunnel) is not support and Help content related to L3 tunnel (IP-IP tunnel) to be removed
	30. <Spec Update> Centralized L2 Tunnel and IP-IP tunnel are not supported
	31. <Spec Update> Remote storage via USB is not supported
4.1.0.2_10204 W 4.1.0.2_10204 R	1. Blank webpage of AP Profile> Configuration SSID on IE browser
	2. LOGIN CAPTIVE PORTAL page that is opened for wireless clients should be the one from CAPTIVE PORTAL SETUP page
	3. Not able to get IPv4/IPv6 address and GUI is not accessible when device is in stateful mode.
	4. Alignment issue in security key for wlan-wizard
	5. Firmware query link to be removed from checklist page (hidden page).
	6. After disconnecting the captive portal session manually from the GUI of the device still able to run the traffic from wlan host without further authentication.
	7. Not able to push configuration among clustering peer group
	8. Graphic missed on webpage of Dashboard> Access Point
	9. Wrong mark on the menu while on the webpage Device Info> Device Status
	10. Wrong mark on the menu while on the webpage Global> SNMP Trap

	11. Wrong mark on the menu while on the webpage USB Settings> USB SharePort
1.01B67_WW 1.01B67_RU	None

Known Issues:

Firmware Version	Known Issues
4.4.1.2_WW 4.4.1.2_RU 4.4.1.1_WW 4.4.1.1_RU	1. 48420 P1 [HQ20150203000014] DWC-2000 Payment Gateway - doesn't show Purchase frame in Captive Portal Login Page 2. P3 [HQ20141204000016]WLAN visualization issues--Not supported for A1 hardware for current image 3. 25281 P2 When IPv6 WAN is configured as static, router is not configuring IP using prefix advertisement(RADVD) from WAN host 4. 26779 P2 'Ap failure status Time out' is not working. 5. 26863 P2 User cannot establish IPSEC VPN tunnel with PFS key "DH-GROUP 17" and "DH-GROUP 18" 6. 26866 P2 Device is not detecting the AD-HOC clients present in its environment. 7. 27677 P3 Device is not authenticating and exchanging routes using second key parameters if first key parameters mismatch in RIP2B/2M 8. 27732 P2 radvd managed flag option use case 9. 27777 P2 The 'other' flag functionality is not working in radvd page 10. 27802 P3 Not possible to configure port speed for option1 from CLI and CLI has commands for LAN port speed also 11. 30052 P3 Device is accepting same subnet for default LAN, VLAN and WAN 12. 30385 P2 PPTP/L2TP client is not getting connected for PPTP/L2TP user with password configured as special characters 13. 30617 P2 There are no fields to configure the client QOS in ssidconfiguration page. 14. 30638 P2 Transparent mode functionality is not working. 15. 35644 P3 [cli]PPTP server/client UserTimeOut Command form CLI is not working properly. 16. 35698 P3 There is no help content for Bandwidth usage and Used applications in DASHBOARD page 17. 35734 P3 logs related to printer are not getting in the GUI and Console

18. 35763 P3 [CLI]Device Accepting 24 characters for sha2-224 integrity algorithm in manual gw policy where as in gui device accepting 28.

19. 35837 P2 Functionality of POLICY BASED LAN QoS policy not working when the profile type is destination UDP port number

20. 35896 P2 Unable to run traffic from device lan/vlan to Access server lan when wan is operating on load balancing.

21. 36684 P2 Unable to establish WDS link if one of the AP is selected as DWL2600 as the configured channel is changing continuously.

22. 38589 P3 UPnP functionality is not working after LAN and WAN restart.

23. 38933 P3 SNMP community field is accepting special characters

24. 40754 P3 No Neighbour APs scanned by 8610 are visible in the device.

25. 40866 P2 Observed that shadow file has the 644 permissions(-rw-r--r--) in shell

26. 40867 P2 Usename and passwords are shown as plaintext in configuration file and db

27. 41190 P2 Temporary users are unable to authenticate even-though account created time and expiry time falls under device time.

28. 41836 P2 Need to support DHCP reserved ip configuration from D-view.

29. 41859 P2 Unable to establish SSLVPN tunnel with java 7 update 51 in linux & windows hosts.

30. 41983 P2 Able to configure the 8610AP to the AP profiile with hardware type as ANY

31. 42023 P3 Need to update the help content for Radio Scheduler supported fields

32. 42033 P2 [CLI] No Options in CLI to Configure IGMP, WDS Groups

33. 42036 P3 Observed operation succeeded message when user tries to add entry with same mac address in MAC Authentication page

34. 42037 P2 [CLI] No option in CLI to configure Firewall--->Blocked Clients

35. 42100 P2 [CLI] Automatic Channel Option in Radio Page Configured from CLI is not reflecting in GUI

36. 42103 P3 No Validation Check for the WEP Key Length

37. 42109 P2 [CLI] No Option to Change Terms of Service Rules of SLA from CLI

38. 42113 P2 [CLI] The fields in Peer configuration page doesn't match with the CLI.

39. 42117 P2 [CLI] Unable to Delete Mac Authentication Client Entry From

CLI

40. 42138 P2 [CLI] SNMP v3 Users List the Authentication Password and PrivacyPassword should be encrypted in CLI

41. 42145 P2 [CLI] No options to upgrade and restore from usb from CLi

42. 42147 P2 [CLI] In CLI there are no options for AP Firmware Download and AP Firmware status

43. 42149 P2 [CLI] Able to Configure NTP Servers with Invalid Domains from Cli

44. 42164 P2 [CLI] Unable to Configure power plan and view status of power plan from CLI.

45. 42179 P2 [CLI] Invalid range for max clients configuration in Distributed Tunnelling in CLI

46. 42185 P1 [CLI] Device is not showing LAN default gateway and host mapping details in CLI

47. 42191 P2 [CLI] Get userdb option is not available in CLI

48. 42193 P2 [CLI] No option to configure List of IPV6 prefix length from CLI

49. 42229 P2 Not able to establish WDS link between 8610 and 8600 Access points.

50. 42265 P2 Need to add support for Multiple user generation from paypal.

51. 42273 P2 Observed that shadow file has the 1151 permissions(-rwxr-xr-x) in shell

52. 42274 P2 Observed password in plain text from the 'teamf1.ascii' file in dbg logs

53. 42300 P2 User not able to edit the added entry in the WDS AP Link List .

54. 42335 P3 The destination hardware type and destination radio type are showing wrong status in WDS link page.

55. 42338 P3 Able to delete WDS group without deleting WDS managed AP entries and wds link

56. 42412 P2 Device is scanning some channels (other than operating channel) even 'Rf Scan other channels' option is disabled

57. 42420 P2 Unable to receive the payment gateway configuration in peer controller when pushed from cluster controller

58. 42421 P2 Unable to receive the SLA configuration in peer controller when pushed from cluster controller

59. 42425 P2 Dissimilarity between the supported radio channels

information provided in 'AP PROFILE RADIO PAGE' and the drop-down
list for Radio-1 in 'EDIT CHANNEL/POWER PAGE'

60. 42459 P2 There is no help content for Firmware via USB page.

61. 42469 P2 After changing vlan captive portal from permanent to
temporary user, authentication type is not displaying correctly in both
GUI and CLI

62. 42562 P2 "show system dashboard" command in cli should show all
the options in GUI

63. 42576 P2 User is unable to add traffic selector with match type as
port-name from cli.

64. 42586 P2 unable to see captive portal and wireless related logs in cli
which are present in gui

65. 42591 P2 [cli]The ip/mac binding rule added from cli is not reflected in
gui

66. 42674 P3 Observed kernel panic when configured IPsec policy with
phase-1 as aes-128/md5 and phase2 as des/sha-512 and dh-group
as group5.

67. 42704 P2 Wireless clients are disconnecting, traffic got stopped after
long duration of traffic when clients(64) are connected using IXWLAN

68. 42729 P2 No option to upload and generate RSA certificates through
CLI

69. 42846 P3 Device is showing "Operation Failed" message while trying to
delete the managed AP profiles.

70. 42876 P2 Device is showing error message as "Operation failed "when
user tries to add multiple payment gateways with same Payment
Receiver Email ID option

71. 42914 P2 User not able to push the wds group configuration from peer
to cluster.

72. 42934 P2 Need to add support for the display of active pptp/l2tp users
in D-view page.

73. 42937 P2 Device is not showing leased IP address of client when it is
connected to roaming AP In distributed tunnelling.

74. 42940 P2 Unable to configure port management option from CLI for
option-1.

75. 42944 P2 WIDS classification page shows threat related status when
two AP's of same MAC address & same ssid are managed from two
different controllers.

76. 42951 P2 Radius accounting functionality is not working, when user

	configured Accounting Server with domain name. 77. 42953 P2 Unable to establish pptp client tunnel with 40-bit MPPE encryption. 78. 43510 P3 There is no help content for few fields in vlan setting page 79. 43935 P2 There is no option to configure facebook Wi-Fi from CLI. 80. 44187 P2 User is able to add more than the scalable limit in the GUI for DHCP reserved,Port-triggering,Firewall,Ip/mac binding pages in New GUI. 81. 44199 P2 WAN1 ddns configuration is not updating for WAN2 in the gui after rollover to wan2 when wan mode is configured as Auto Rollover. 82. 44204 P2 User is able to delete the resources which are in use by SSL policies 83. 44205 P3 Device is throwing improper error message when user try to add the resource with the existed resource name. 84. 41937 P2 Status of server checking is not displaying until refreshing page 85. 38572 P3 In CLI there are no commands to configure openvpn 86. 41997 P2 Able to add AP profile name with special characters from CLI 87. 42404 P2 No error message displayed while configuring invalid subnet mask through CLI. 88. DBG15080002 The "Select All" button is not functional on discovery page, thus we can't manage all AP in a once. (v4412)
4.4.0.2_B301_WW 4.4.0.2_B301_RU	1. [25560][DBG12050195] "In some web pages (ex AP Profile_Radio), devices does not show 'Operation Successfully' after save settings. 2. [31946][DBG12050169] "DWC WEB GUI still logout after some time operation (randomly), needs to login again to use." 3. [24510][DEUR20121022000001][HQ20121023000001] Guest privilege 4. [40950] - Captive portal page not showing forced login page for already login users. 5. [33701] - Able to access corresponding websites if we block Violence / Undesirable, Government Blocking List, Remote Control/Desktop and Crime / Terrorism categories 6. [33603] - User is able to access the blocked sites which are configured in Category filtering page using proxy sites 7. [24340] - SSL tunnel is getting dropped after around 8 minute of continuous traffic.Device Name & Model DLink & DWC 1000 8. [DEUR20140522000001][HQ20140523000004] DWC-1000 - CP time

	doesn't count down in browser after logging b. In View Accounts page of FrontDesk, after pressing the "F5" or refresh button in IE11 browser, the FrontDesk user is re-directing to login page (get logged out). (v4302 didn't include this IE11 support enhancement) 9. [47747] Radio1 mode is getting into 802.11a/n mode after changing the country code. 10. [47749] Clients status page is not displaying 802.11ac clients.
4.3.0.2_B401_WW 4.3.0.2_B401_RU	1. [47747] Radio1 mode is getting into 802.11a/n mode after changing the country code. 2. [47749] Clients status page is not displaying 802.11ac clients.
4.3.0.2_WW 4.3.0.2_RU	1. [25560][DBG12050195] "In some web pages (ex AP Profile_Radio), devices does not show 'Operation Successfully' after save settings. 2. [31946][DBG12050169] "DWC WEB GUI still logout after some time operation (randomly), needs to login again to use." 3. [24510][DEUR20121022000001][HQ20121023000001] Guest privilege 4. [40950] - Captive portal page not showing forced login page for already login users. 5. [33701] - Able to access corresponding websites if we block Violence / Undesirable, Government Blocking List, Remote Control/Desktop and Crime / Terrorism categories 6. [33603] - User is able to access the blocked sites which are configured in Category filtering page using proxy sites 7. [24340] - SSL tunnel is getting dropped after around 8 minute of continuous traffic.Device Name & Model DLink & DWC 1000 8. [DEUR20140522000001][HQ20140523000004] DWC-1000 - CP time doesn't count down in browser after logging b. In View Accounts page of FrontDesk, after pressing the "F5" or refresh button in IE11 browser, the FrontDesk user is re-directing to login page (get logged out). (v4302 didn't include this IE11 support enhancement)
4.3.0.1_WW 4.3.0.1_RU	1. [25560][DBG12050195] "In some web pages (ex AP Profile_Radio), devices does not show 'Operation Successfully' after save settings. 2. [31946][DBG12050169] "DWC WEB GUI still logout after some time operation (randomly), needs to login again to use." 3. [24510][DEUR20121022000001][HQ20121023000001] Guest privilege 4. [40950] - Captive portal page not showing forced login page for

	already login users.
	7. [33701] - Able to access corresponding websites if we block Violence / Undesirable,Government Blocking List,Remote Control/Desktop and Crime / Terrorism categories
	8. [33603] - User is able to access the blocked sites which are configured in Category filtering page using proxy sites
	9. [24340] - SSL tunnel is getting dropped after around 8 minute of continuous traffic.Device Name & Model DLink & DWC 1000
	10. OpenSSL CCS Injection vulnerability (man-in-the-middle attack)
	Reference: CVE-2014-0224
	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224
	https://www.openssl.org/news/secadv_20140605.txt
	Solution: We will update OpenSSL patch to 0.9.8za that addresses the vulnerability on next hotfix, say DWC-1000_FW_4.3.0.1_B101 or DWC-1000_FW_4.3.0.2.
4.2.0.6_WW 4.2.0.6_RU	1. [25560][DBG12050195] "In some web pages (ex AP Profile_Radio), devices does not show 'Operation Successfully' after save settings.
	2. [31946][DBG12050169] "DWC WEB GUI still logout after some time operation (randomly), needs to login again to use."
	3. [24510][DEUR20121022000001][HQ20121023000001] Guest privilege
	4. RAIUDS Accounting feature issue

Related Documentation:

- DWC-1000 User Manual ver.1.01
- DWC-1000 CLI Reference Guide ver. 1.01