Firmware Version: V1.13.04
Prom Code Version:
Published Date: 2016/7/19

Content:

Upgrading Instructions: 2
New Features: 2
Problems Fixed: 4
Known Issues: 5
Related Documentation: 5

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
v1.13.04	2016/7/19	DCS-932L	A1,A2
v1.12.02	2015/10/22	DCS-932L	A1,A2
v1.11.03	2015/9/2	DCS-932L	A1,A2
v1.10.03	2015/2/6	DCS-932L	A1
v1.09_b1	2014/4/11	DCS-932L	A1
v1.08_b2	2014/3/24	DCS-932L	A1
v1.07_b2	2013/12/26	DCS-932L	A1
v1.06_b4	2013/2/20	DCS-932L	A1
v1.05_b5	2012/11/19	DCS-932L	A1
v1.04_b5	2012/9/3	DCS-932L	A1

Upgrading Instructions:

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the D-Link website. The file is in .bin file format.
2. Log-in camera web UI and enter setup/Maintenance/Firmware upgrade
3. Click Browse… and specify the firmware file.
3. Click Upgrade. The camera starts to upgrade and will reboot automatically when the upgrade completes.

New Features:

Firmware Version	New Features
v1.13.04	1. Upgrade mydlink agent to 2.1.0-b27. 2. Change the HTTPs self-signed certificate to SHA2 algorithms. 3. Support Mydlink UID mechanism (mdb get dev_uid) 4. Change the support page hyperlink of Firmware Upgrade web-UI to www.dlink.com. 5. Updated OpenSSL to v0.9.8o. 6. Remove mDNSResponder daemon on the unit. 7. Remove the Bonjour settings from the Network Setup web-UI. 8. Change the default system time to 2016-01-01 9. Update the years in the copyright statement for IP Camera's web-UI to 2016.

	10. Add authentication to CGI /config/stream_info.cgi. 11. Offer the password validation on console port. (Console's Password is synchronized with the admin's password)
V1.12.02	1. Update mydlink agent to v2.0.19-b35n. 2. The ActiveX and Java Applet signing certificate are updated.
V1.11.03	1. Update mydlink agent to 2.0.19-b35 2. Add the login check mechanism to solve Brute Force Attack issue 3. Change LED blinking time on WPS error/timeout to 10 seconds. 4. Add Hardware Version item on the Status page of the camera's web-GUI.
V1.10.03	1. Upgrade mydlink agent to v2.0.18-b61 2. Remove SSL, change to support TLS.
V1.09_b1	1. Update mydlink agent to 2.0.17-b60 for fixing mydlink notification fail issue.
V1.08_b2	2. New mydlink agent 2.0.17-b55. 3. Change the default FTP to passive mode. 4. Change WPS LED on 10 seconds after WPS succeed. 5. Change LANDAP protocol's password length to 0-32 characters. 6. Change copyright from [2012-2013] to [2012-2014]. 7. Change camera default time from [2013-01-01] to [2014-01-01]. 8. Support Win 8.1 + IE 11. 9. Support Java 7 Update 51. 10. SSL Certificate will be automatically self signed (regenerated) during initial configuration/factory reset.
V1.07_b2	1. Add schedule feature for motion detection function. 2. NTP source port change to port 123 3. Add user can configure interval setting for motion detection of mail/ftp. 4. User account name is limit as: 0-9, a-z, A-Z, ".", "-", "_". 5. Update Mydlink agent to v2.0.17-b31 6. Limit "Auto" FTP image frequency not over 5 frames/second.
V1.06_b4	**Firmware V1.06_b4 is only supported by wizard v1.02.10 or above.** 1. Change maximum admin password length, from 8 characters to 30 characters. 2. Change PPPoE retry timing, retry connection on 30 seconds interval till connect. 3. New ActiveX to support long admin password. 4. Default time change to 2013-01-01 5. Change IR LED Night to Day switch timing to 7 seconds.
V1.05_b5	1. Add mydlink agent version displayed on Web UI. 2. Update Java program to support new mjpeg streaming format

	3. Change NTP request timing
v1.04_b5	1. Upgrade new mydlink agent to v2.0.16-b4 2. Secure the configuration file with the new changed encryption method. 3. Remove two WebGUI Hidden Pages for RD develop using. 4. Remove the Telnet Daemon will be activated about 5 seconds when the Device is booting. 5. Remove the hidden FTP server.

Problems Fixed:

Firmware Version	Problems Fixed
v1.13.04	1. Fixed CSRF vulnerability for the camera's web-UI (Exclude CGI APIs). 2. Fixed the "RSA-CRT key leaks" vulnerability. 3. Fixed the "LANDAP stack overflow" vulnerability. (discovered by search SEARCH-LAB) 4. Remove the "Arbitrary file upload interface" vulnerability. (discovered by search SEARCH-LAB) 5. Fixed an issue that Time zone setting for Minsk should be GMT+3. 6. Fixed a vulnerability - Authenticated Arbitrary File Upload with Root Privileges. (discovered by IOActive Security) 7. Fixed a vulnerability - Authenticated Root OS Command Injection in File Upload. (discovered by IOActive Security) 8. Fixed an XSS vulnerability - Stored XSS in User Name. (discovered by IOActive Security) 9. Fixed an XSS vulnerability - Reflected XSS in HTTP Host Header. (discovered by IOActive Security)
V1.11.03	1. Fixed the IE11 compatibility issue in Windows 10. 2. Change WPS LED behavior blinking time on WPS error/timeout to 10 seconds. 3. Add the pop-up warning message when the user creates an existing user account on Device Web GUI. 4. Support to auto-create FTP folder if the folder doesn't exist on FTP server. 5. Fixes a vulnerability is found in Korea that a hidden page can enable the Telnet service in the device. 6. Fixed HTTPS issue that cause Day/Night control not work from portal/app 7. Fixes the issue in which IP Cam cannot create FTP folder with FTP server on

	Netgear R7000 Router. 8. Fixed CGI /reset.cgi reboot command not work issue 9. Modify Time Zone Table list to support some existing time zones changes.
V1.07_b2	1. Fixed ip task will be restarted issue on DHCP renew time. 2. Fixed E-mail/FTP cannot be started issue if motion detection is enabled first. 3. Fixed UpnP issue with DIR-826L router 4. The max length of Admin password change to 32 characters
V1.05_b5	1. Fixed ios6 live view hang issue – modify mjpeg streaming format 2. Fixed sometimes startup java view failed on Win 7 + IE9 3. Fixed live view issue if http port is changed to 12345. 4. Fixed live view streaming cannot pass through router's virtual server. 5. Fixed e-mail loss issue when live view the camera.
v1.04_b5	1. Fixed the live stream can't display when using the https connection. 2. Fixed bad audio streaming on 3G internet access.

Known Issues:

Firmware Version	Known Issues

Related Documentation:

N/A