



**Firmware Version:** v2.14.04  
**Prom Code Version:**  
**Published Date:** 2016/10/18

---

**Content:**

Upgrading Instructions:..... 2  
New Features:..... 2  
Problems Fixed: ..... 3  
Known Issues: ..... 4  
Related Documentation: ..... 4

## Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
v2.14.04	2016/10/18	DCS-932L	B1,B2
V2.13.15	2016/7/20	DCS-932L	B1,B2
V2.12.01	2015/10/22	DCS-932L	B1,B2
V2.11.03	2015/9/1	DCS-932L	B1,B2
V2.10.03	2015/6/29	DCS-932L	B1
V2.01.03	2015/2/6	DCS-932L	B1
V2.00b6	2014/7/2	DCS-932L	B1

## 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
v2.14.04	<ol style="list-style-type: none"> <li>1. Upgrade mydlink agent to 2.1.0-b41.</li> </ol>
V2.13.15	<ol style="list-style-type: none"> <li>1. Upgrade mydlink agent to 2.1.0-b27.</li> <li>2. Change the HTTPs self-signed certificate to SHA2 algorithms.</li> <li>3. Support Mydlink UID mechanism (mdb get dev_uid)</li> <li>4. Change the support page hyperlink of Firmware Upgrade web-UI to <a href="http://www.dlink.com">www.dlink.com</a>.</li> <li>5. Updated OpenSSL to v0.9.8o.</li> <li>6. Remove mDNSResponder daemon on the unit.</li> <li>7. Remove the Bonjour settings from the Network Setup web-UI.</li> <li>8. Change the default system time to 2016-01-01</li> <li>9. Update the years in the copyright statement for IP Camera's web-UI to 2016.</li> <li>10. Add authentication to CGI /config/stream_info.cgi.</li> <li>11. Offer the password validation on console port. (Console's Password is synchronized with the admin's password)</li> </ol>

V2.12.01	<ol style="list-style-type: none"> <li>1. Update mydlink agent to v2.0.19-b54n.</li> <li>2. The ActiveX and Java Applet signing certificate are updated.</li> </ol>
V2.11.03	<ol style="list-style-type: none"> <li>1. Update mydlink agent to 2.0.19-b54</li> <li>2. Add the denoise mechanism to reduce the background noise</li> <li>3. Add the login check mechanism to solve Brute Force Attack issue</li> <li>4. Add Hardware Version item on the Status page of the camera's web-GUI.</li> <li>5. Change the model and model number of the UPnP properties.  <a href="#">F/W V2.11.03 only supports D-ViewCam version as below or above.</a> <ol style="list-style-type: none"> <li>1. <a href="#">DCS-100 V3.6.5 + DP V1.6.13</a></li> <li>2. <a href="#">DCS-100 V4.0.4 + DP V2.0.15</a></li> </ol> </li> </ol>
V2.10.03	<ol style="list-style-type: none"> <li>1. Update mydlink agent to v2.0.19-b35.</li> <li>2. Support auto image setting switching mechanism for H/W B1 and B2 (or above) camera lens. (*H/W B2 or above only supports v2.10.03 or above)</li> </ol>
V2.01.03	<ol style="list-style-type: none"> <li>1. Upgrade mydlink agent to v2.0.18-b61</li> <li>2. Remove SSL, change to support TLS.</li> </ol>
V2.00b6	<p>Initial version.  <a href="#">F/W v2.00 is not backward compatible to H/W Ax version.</a></p>

## Problems Fixed:

Firmware Version	Problems Fixed
v2.14.04	<ol style="list-style-type: none"> <li>1. Fixed an issue that Mydlink service will be off line when FW upgrade to v2.13.15.</li> </ol>
V2.13.15	<ol style="list-style-type: none"> <li>1. Fixed CSRF vulnerability for the camera's web-UI (Exclude CGI APIs).</li> <li>2. Fixed the "RSA-CRT key leaks" vulnerability.</li> <li>3. Fixed the "LANDAP stack overflow" vulnerability. (discovered by search SEARCH-LAB)</li> <li>4. Remove the "Arbitrary file upload interface" vulnerability. (discovered by search SEARCH-LAB)</li> <li>5. Fixed an issue that Time zone setting for Minsk should be GMT+3.</li> <li>6. Fixed a vulnerability - Authenticated Arbitrary File Upload with Root Privileges. (discovered by IOActive Security)</li> <li>7. Fixed a vulnerability - Authenticated Root OS Command Injection in File Upload. (discovered by IOActive Security)</li> <li>8. Fixed an XSS vulnerability - Stored XSS in User Name. (discovered by IOActive Security)</li> </ol>

	<ol style="list-style-type: none"> <li>9. Fixed an XSS vulnerability - Reflected XSS in HTTP Host Header. (discovered by IOActive Security)</li> </ol>
V2.11.03	<ol style="list-style-type: none"> <li>1. Fixed the IE11 compatibility issue in Windows 10.</li> <li>2. Change WPS LED behavior blinking time on WPS error/timeout to 10 seconds.</li> <li>3. Remove the reboot function by pressing and holding the reset button in less than 3 seconds.</li> <li>4. Add the pop-up warning message when the user creates an existing user account on Device Web GUI.</li> <li>5. Support to auto-create FTP folder if the folder doesn't exist on FTP server.</li> </ol>
V2.10.03	<ol style="list-style-type: none"> <li>1. Fixed HTTPS issue that causes Day/Night control not work from portal/app.</li> <li>2. Fixes the issue in which IP Cam cannot create FTP folder with FTP server on Netgear R7000 Router.</li> <li>3. Fixed CGI /reset.cgi reboot command not work issue.</li> <li>4. Modify Time Zone Table list to support some existing time zones changes.</li> </ol>

### Known Issues:

Firmware Version	Known Issues

### Related Documentation:

N/A