



**Firmware Version:** V3.02  
**Prom Code Version:**  
**Published Date:** 2016/01/25

**Content:**

Upgrading Instructions:..... **Error! Bookmark not defined.**  
New Features: ..... 2  
Problems Fixed: ..... 2  
Known Issues: ..... 3  
Related Documentation: ..... 3

## Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
V1.00	2010/12/22	DCS-7110	A1
V1.10	2012/8/01	DCS-7110	A2
V1.20	2012/8/31	DCS-7110	A3
V3.00	2013/1/9	DCS-7110	B1
V3.01	2015/10/15	DCS-7110	B1
V3.02	2015/01/25	DCS-7110	B2

## Upgrading Instructions:

Follow the steps below to upgrade the firmware:

1. Log-in camera web UI and enter setup/Maintenance/Firmware upgrade
2. 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:

Fireware Version	New Features
V1.10	Support PPPoE CHAP.
V1.10	Approval by ONVIF test tool v1.02.4.
V1.20	Support NIPCA motion detection cgi.
V3.00	<ol style="list-style-type: none"> <li>1. Support 1920x1080 for HW B1 version.</li> <li>2. Camera Name &amp; Page Title change to 64 Bytes.</li> </ol>

## Problems Fixed:

Firmware Version	Problems Fixed
V1.10	<ol style="list-style-type: none"> <li>1. D-Track no. DBG11060237 &amp; DRU20110614000005, camera doesn't respond by the default IP address.</li> <li>2. Image noise issue in night mode.</li> </ol>
V1.20	<ol style="list-style-type: none"> <li>1. DBG10120098 : Add default icon in Image Settings (Profile 1).</li> <li>2. DBG11110304 : After disable DUT HTTPS secure connection, DUT redirect to HTTP webpage with HTTPS port.</li> <li>3. DBG11110317 : After change logo graph, the title name would overlap the left logo graph in live view page.</li> <li>4. DBG11110318 : The copy button in HTML Code Examples page didn't work.</li> </ol>

	<p>5. DBG12010013: When change DUT HTTP/RTSP port to 8081/5544, browse DUT H.264 using QuickTime plugin HTML code example by Firefox would show connection failed.</p> <p>6. DBG11100155 : After firmware upgrade the logo graph settings would disappear.</p> <p>7. DBG11100146 : Recording notify message file didn't show the right folder path of network storage server. (Remove the path information)</p> <p>8. DBG11110280 : The values of default and output frame size setting cannot be synchronized.</p>
V3.00	<p>1. Change CBR max. option from 6M to 8M for saving bandwidth.</p> <p>2. IR sometimes has inconsistent situation. (Display shows Day mode, IR LEDs are ON at the same time)</p> <p>3. When create HTTPS certification, popup Certificate Request window has chance to show can't find home page.</p> <p>4. Remove "one hour" in updating interval of NTP.</p>
V3.01	<p>1. Change to 2015 version Digital Signature.</p> <p>2. Security holes issues.</p> <ul style="list-style-type: none"> <li>a. RTSP authentication.</li> <li>b. Slowloris HTTP DoS.</li> <li>c. Password Stored in Web Page.</li> <li>d. Open SSL binary transmitting.</li> </ul> <p>3. Disable SIP port, FTP port, SSL v3.0.</p> <p>4. Change RTSP default authentication to Basic.</p> <p>5. Show alert message if User use Chrome v45 and above.</p>
V3.02	<p>1. Change default streaming for Chrome use "MJPEG".</p> <p>2. Update Windows IE plugin for SHA2 certification. (ActiveX)</p> <p>3. Security holes issues Fix:</p> <ul style="list-style-type: none"> <li>a. Update OpenSSL Library to 1.01h</li> <li>b. Fix TLS/SSL Server Supports Weak Cipher Algorithms</li> <li>c. Add CSRF protection</li> <li>d. Change RTSP authorization.</li> <li>e. Clear useless handle event message log post.</li> <li>f. Fix Brute Force attack</li> </ul>

## Known Issues:

Firmware Version	Known Issues
V3.00	<p>1. DBG13120167: Stopped working in IE10 browser during endurance test.</p> <p>2. DBG13120169: DCS-100 often disconnected to DUT and recording discontinuously during endurance test.</p> <p>3. DBG13120173: The endurance test recording uploaded to SMB server DNS-1200-5 would lag.</p>
V3.01	<p>1. Security Holes</p> <ul style="list-style-type: none"> <li>a. SSL / TLS Renegotiation DoS</li> <li>b. WebVideoActiveX Integer Overflow</li> <li>c. Unvalidated Redirects</li> <li>d. Command Injection</li> <li>e. Cross Site Scripting</li> <li>f. TLS update to v1.2</li> <li>g. OpenSSL CCS Injection</li> <li>h. CSRF option</li> <li>i. RTSP can't support VLC</li> <li>j. Change Brute force attack blocking time to 5 min</li> </ul>

**Related Documentation:**

---

N/A