



Firmware Version: 2.21.B021

Published Date: Feb. 21, 2022

Copyright © 2022

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:

Revision History and System Requirement:	3
Upgrading Instructions:	3
New Features:	4
Problem Fixed:	4
Known Issues:.....	5
Related Documentation:	6

Revision History and System Requirement:

Firmware Version	Date	Model	Hardware Version
2.21.B021	Feb 21 2022	DBG-2000	A1
2.20.B073	Aug 20 2021	DBG-2000	A1

Upgrading Instructions:

When the device added to Nuclias portal, the Nuclias portal will automatically update the Business Gateway firmware to the latest version. User can go to SETTINGS ->Firmware -> Model

UPGRADE to change the firmware upgrade policy and there are three options:

The screenshot shows the Nuclias portal interface for firmware management. At the top, there is a navigation bar with links: DASHBOARD, MONITOR, CONFIGURE, REPORTS, SETTINGS, and HELP. Below this, the breadcrumb path is 'Settings / Firmware'. There are three tabs: 'NEW RELEASES', 'FIRMWARE UPGRADES' (which is active), and 'FIRMWARE MANAGEMENT'. Under the 'FIRMWARE UPGRADES' tab, there are two sub-tabs: 'SCHEDULE UPGRADES' (active) and 'BULK UPGRADES'. The main content area contains a form with the following elements:

- Device model:** A dropdown menu currently set to 'DBG-2000'.
- Firmware availability:** A text input field containing 'Update available / Up to date'.
- Preview:** A button with a document icon and the text 'Preview'.

New Features:

Firmware Version	New Features
2.21.B021	<ol style="list-style-type: none"> 1. Cloud Bulk-import support 2. Add connect/disconnect buton for PPTP/L2TP/OpenVPN 3. IPsec backup policy 4. IPsec Keep alive 5. SMTP ALG 6. All available WAN interface can be configured for different features 7. IPsec FQDN can select from DDNS 8. WCF splash page support
2.20.B073	<ol style="list-style-type: none"> 1. The first release

Problem Fixed:

Firmware Version	Problems Fixed
2.21.B021	<ol style="list-style-type: none"> 1. Allow Ping from LAN is having no effect on traffic from LAN and DMZ HQ20211216000005 2. Unable to establish Ipsec tunnel using local auth if one policy uses Local authentication and other vpn policy is for radius. VBG21050038 3. OPENVPN_OMNISSL_AUTH_SUCCESS and AUTH_FAIL EVENT LOGS VBG21050093 4. Device is not sending FAIL events for IPsec VPN VBG21060019 5. PnP port mapping list won't be cleared DBG21070653 6. [Vulnerability] Web server doesn't have 'X-Content-Type-Options' Header VBG21080067 7. [Vulnerability] Webs erver's Content-Encoding header setting is risky & vulnerable to Breach attack. VBG21080068 8. mnissl portal login event logs fix VBG21090078 9. Resrticting device reboot during firmware upgrade VBG21090079 10. Wins and Split dns configuration must be in global setting VBG21090081 11. User should be able to download Debug Logs from Local UI VBG21090082 12. Incorrect error message for wrong old password during password change VBG21090084

	<p>13. Auto-rollover wan-mode functionality is not work perporly VBG21110056</p> <p>14. In load-balancing wan mode, DDNS functionality is not work properly. VBG21110062</p> <p>15. IPSEC Event and Status changes for l2tp over ipsec. VBG21110083</p> <p>16. LDAP authentication server with TLS enabled to captive portal is not work. VBG21110093</p> <p>17. Device is getting ethernet port is connected event even when device is in idle state. HQ20211209000005</p> <p>18. LAN3 default setting not show DHCP client. HQ20211209000004</p> <p>19. Device reports ghost client data. HQ20211215000008</p> <p>20. local WebUI doesnt respond and it won't be managed after factory reset. HQ20211223000006</p> <p>21. [Vulnerability] The anti-clickjacking X-frame-options HTTP header is not present. VBG21080065</p> <p>22. [Vulnerability] Webserver doesn't have X-XSS protection header. VBG21080066.</p>
--	---

Known Issues:

Firmware Version	Known Issues
2.21B021	<ol style="list-style-type: none"> 1. NAT lookback is not work. 2. Netbios over Ipsec is not yet supported 3. IGMP PROXY working only on one of the base interfaces after restart of IGMP service. 4. L2TP over IPsec is not working when WAN mode is in Auto-rollover. 5. External authentication servers are not working for mschap,ms-chapv2 authentication protocols in pptp and l2tp vpn. 6. WCF https blocking are not redirected to WCF warning page. 7. Unable to download Client configuraton in IE11 Browser windows 7 (64bit) from OMNISSL PORTAL. 8. Incorrect CP redirection page in safari and IE browsers for custom splash page. 9. External authentication servers are not working for mschap,ms-chapv2 authentication protocols in pptp and l2tp vpn

Related Documentation:

- DBG-2000 User Manual v2.20.08
- DBG-2000 A1 Quick Installation Guide 1.00