DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

Firmware Release Notes
Digi Passport
Version 1.5.2 (March 24, 2022)

INTRODUCTION

This is the production release of firmware for the Digi Passport. These devices provide console management access to various servers, devices, and systems that may be accessed by a serial cable to a console port. These devices feature console management through a console menu or web interface to allow configuration of network settings, serial settings, administration settings, and user settings. High-end features include Telnet/SSHv1/SSHv2/RawTCP protocols, Local, RADIUS, TACACS+, and LDAP authentication, Port logging through Local, NFS, Samba, Syslog and Memory cards, PCMCIA slot and configuration, custom menus, keyword monitoring and SMTP/SNMPv3 notification, IPMI 2.0, Samba, IPv6, PPP, USB, Peer to Peer Clustering, Syslog-NG, Encrypted RealPort, freeKVM, Perl scripting, Dual 10/100 mbps Ethernet network interface, and Digi Discovery server to allow discovery and network configuration from the Digi Discovery Applet.

SUPPORTED PRODUCTS

- Digi Passport 4
- Digi Passport 8
- Digi Passport 16
- Digi Passport 32
- Digi Passport 48

KNOWN ISSUES

None

KNOWN LIMITATIONS

- Shell-in-a-box does not allow multi-line copy and paste.
- Using cancel button when removing Custom Menus or Copying custom menus causes the page to be submitted and the menus removed or copied, respectively. To cancel without causing this effect, use the browser's Back button.
- If there are a large number of slave units configured the Master can take up to 8 minutes to boot up.

ADDITIONAL INFORMATION

When using the SUN Java Runtime Environment in Windows, you may need to verify the browser you are using has been enabled with the Java plug-in. To verify, use the following steps:

1. Go to Control Panel in Windows (may be accessed through My Computer or Start menu)
2. If you are using "Category View", click "Switch to Classic View".
3. Click Java Plug-In icon. (if this icon does not exist, verify JRE is correctly installed)
4. Click on the "Basic" tab.
5. Verify "Enable Java Plug-In" is checked.
6. Click on the "Browser" tab.
7. Verify appropriate browser or browsers are checked.
8. Click on the "About" tab.
9. Verify Java Plug-in version is 1.3 or later.

freeKVM: To use the freeKVM features it is necessary to have Java properly installed for your browser (as per the above specifications) and to have the necessary software installed in the PATH on your workstation. Detailed instructions are included in the Passport Product manual.

UPDATE CONSIDERATIONS

In order to add compliance with California's Senate Bill No. 327, for information privacy of connected devices, the handling of the root password for newly manufactured products is changing.

Products manufactured after January 1, 2020 will no longer use a fixed, default root password. Rather, a per-device, unique password will be assigned during manufacturing, and will be visible on a product label. It will still be possible to change the password for the root user on a per-device basis.

Admin user: The admin user is inactive in the new firmware. To activate the admin user, you must first assign a password to the admin user.

Products manufactured prior to the adoption of the new product labeling are grandfathered in and will continue to operate as before.

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update production devices.
2. Unless otherwise noted, apply updates in the following order:
    a. Device firmware
    b. Modem firmware
    c. Configuration
    d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, go to https://www.digi.com/products/iot-platform/digi-remote-manager. If you prefer manually

updating one device at a time, follow these steps from the manual:

1. Firmware update process

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, and knowledge base and peer-to-peer support forums. Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 1.5.2 March 24, 2022

This is a mandatory release.

MD5 Checksum
dd11fb9d730ab22c7f6fe8c5f1e07d38

SHA-256
7d8a88bdbae2b5b2fb423d464e834aff461dd8fb80b83f997c775d4237e7d8be

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

CVE-2022-26952
CVE-2022-26953

Improvements have been made to the web server to address how requests were being handled. Two buffer overflow vulnerabilities (resulting in denial of service) have been resolved.

BUG FIXES

None

VERSION 1.5.1.1 June 05, 2020

This is a mandatory release.

MD5 Checksum
FAD484506B7CF36D6E97481D94C02E9E

SHA-256

4747A6C10F5BE6F703EDB17B63857405835135E7031C6F1F789

24DF7A2FAC19A

NEW FEATURES

None

ENHANCEMENTS

None

SECURITY FIXES

CVE-2020-8597

https://nvd.nist.gov/vuln/detail/CVE-2020-8597

pppd (Point to Point Protocol Daemon) versions 2.4.2 through 2.4.8 are vulnerable to buffer overflow due to a flaw in Extensible Authentication Protocol (EAP) packet processing in eap_request and eap_response subroutines.

Due to a flaw in the Extensible Authentication Protocol (EAP) packet processing in the Point-to-Point Protocol Daemon (pppd), an unauthenticated remote attacker may be able to cause a stack buffer overflow, which may allow arbitrary code execution on the target system. This vulnerability is due to an error in validating the size of the input before copying the supplied data into memory. As the validation of the data size is incorrect, arbitrary data can be copied into memory and cause memory corruption possibly leading to execution of unwanted code.

BUG FIXES

None

VERSION 1.5.1 November 20, 2019

This is a mandatory release.

NEW FEATURES

1. Added support for California's Senate Bill No. 327. Product manufactured after January 1, 2020 will have a unique password.

ENHANCEMENTS

None

SECURITY FIXES

Researchers have discovered new denial-of-service (DoS) vulnerabilities in Linux and FreeBSD kernels, including a severe vulnerability called SACK Panic that could allow malicious actors to remotely crash servers and disrupt communications, according to an advisory.

“The vulnerabilities specifically relate to the Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed “SACK Panic,” allows a remotely-triggered kernel panic on recent Linux kernels,” the advisory stated. This vulnerability also goes back a long time (since Linux v2.6.29, that was released 10 years ago).

"The issues have been assigned multiple CVEs: CVE-2019-11477 is considered an Important severity, whereas CVE-2019-11478 and CVE-2019-11479 are considered a Moderate severity".

BUG FIXES
None

VERSION 1.5.0 September 10, 2017

- added ability to see alternative Port IP on the port config page.
- added the addp client binary
- added Security updates
- added GCM ciphers
- added Shellinabox to replace java jta
- added improvements so the web session ID is not guessable
- added Secure WEB and credentials
- added LLDP support
- Fixed a problem where you could not upgrade the firmware from the /mnt/flash directory
- Fixed Java issues
- Fixed a problem where there was no default route for eth1 when source based routing was enabled
- Fixed a problem with failover for TACACS
- Fixed a problem where a manually added route was being removed from routing table when connected to serial port
- Updated the cert dates for TLS/SSL and Java
- Fixed a problem where you couldn't access the device via HTTPS using Firefox or the Edge browser
- Fixed issues with Certificate generation
- Fixed a problem where sometimes you were required to login to the Web UI twice
- Fixed a problem with the Copyright date in the Web UI
- Fixed a problem where the CLI would sometimes lockup when accessed via SSH
- Fixed a problem where DHCPv6 didn't work

VERSION 1.4.4.3 October, 2014

- Fixed several security issues PP-47: CVE-2014-6271 / CVE-2014-7169 CVE-2014-7186 / CVE-2014-7187 CVE-2014-6277 / CVE-2014-6278 (bash security reported vulnerabilities)
- Fixed a security issue PP-50: CVE-2014-3566 (SSL reported vulnerability)

VERSION 1.4.4 October, 2013

- Added ability to display hostnames rather than IP's for peer units.
- Added ability for power status to be written to syslog automatically.
- Added Xmodem upload script to system.
- Fixed a bug causing Passport lockups.

- Fixed an Error in MIB file.
- Fixed a problem where Admin user could not change password from configmenu.
- Fixed a problem where server refused to allocated pty message at boot time.
- Updated Java signatures.
- Fixed a problem where USB service wouldn't recover after accidental removal.
- Fixed a problem where you couldn't monitor users logged in via SNMP.
- Fixed a problem where Kerberos fails if entering hosts greater than 15 characters via web or CLI.

VERSION 1.4.3 January, 2013

- Updated the version of powerman to 2.3.16
- Updated SNMP to allow an address of 0.0.0.0 to work with any SNMP browser.
- Added telnet support to powerman.
- Improved the response time when adding power controllers.
- Fixed a problem where Powerman ignores and does not negotiate telnet parameters.
- Fixed a problem with randon port lockups.
- Fixed a problem where Configuration files can get corrupted under various conditions.

VERSION 1.4.2 July, 2012

- Increased the serial port inactivity timeout to 24 hours.
- Increased the security of the SSL ciphers.
- Added "portmgmt" command to kick users off of ports.
- Fixed a problem where you couldn't add a remote port via stanzamenu.
- Fixed a problem handeling large files.
- Fixed a problem that caused slow web ui response.
- Fixed a problem where an external modem would only answer on the 2nd ring.

VERSION 1.4.0 June, 2011

- Set the Port mgmt option always on if override is selected.
- Added support for the APC power controllers.
- Added support for a configurable time limit setting once a user account is locked out.
- Added option to "supress connection announcements"
- Added support for stanza based configuration
- Fixed a problem where we were Unable to import a config file created via auto backup.
- Fixed a problem that caused random port lock ups.
- Fixed a problem where port logging does not create backup files once specified.
- Fixed a problem When you are managing a Power Group through Configmenu you can't see the status of the outlets
- Fixed a problem that caused a delay accessing telnet ports.
- Fixed Do not allow slashes within the port title.

VERSION 1.3.0.2 February, 2011

- Fixed a problem which caused intermittent factory resets and reboots.

VERSION 1.3.0 June, 2010

- Added ability to notify new sniff session of existing sessions.
- Added support for CIDR blocks for IP filtering.
- Added an option to save and use User's custom iptable rules.
- Improved telnet performance when a ServerTech power Controller is configured on the device.
- Added the ability to save custom /etc settings to a custom directory in /usr2.
- Added an option in the Web UI to save custom settings to the custom directory in /usr2.
- Added a timer variable option for power polling interval of power controllers
- Fixed a problem with sending a serial break through an SSH tunnel.
- Fixed a problem where adding slaves to a cluster would cause other salves to disappear.
- Fixed a problem with the NAS-IP attribute for Radius authentication.
- Fixed a problem where multiple port connections could cause high system load.

VERSION 1.2.4 August, 2009

- Added enhancements to the powerctrl command
- Added the ability to see the clusterd slave units title in the portaccess menu
- Added enhancements to the autofwup command
- Added enhancements to Netcat
- Fixed a problem with SNMP and multuple power strips
- Fixed a problem with assigning user permissions to an outlet if not linked to a serial port.
- Fixed a problem with rebooting outlets in a power group
- Fixed a problem where a outlet title would not show up in the power management page.
- Fixed a problem where the power trap always sent power off
- Fixed a problem with user permissions and outlet control

VERSION 1.2.0 October, 2008

- Added hotkey access to port logs.
- Added support for Raw TCP to the java web applet.
- Added support for multiple FreeKVM entries per port.
- Added support for search functionality to PortAccess Menu.
- Enhanced Keyword search functionality.
- Enhanced PPP functionality when authentication is disabled.
- Enhanced syslog server functionality.
- Added Push functionality to Clustering.

- Added support for multiple email recipients for alerts.
- Added ability to import configuration via SNMP.
- Added ability to clone ports.
- PPP enhancements.
- Added ability to assign names to Clusters.
- Enhanced paging functionality in Web UI.
- Added functionality to display auto configured IPv6 address in Web UI.
- Added ability to enable/disable SSL 2.0 and 3.0.
- Added network bridging.
- Added ability to configure Power rights for multiple outlets at the same time.
- Fixed a problem with source based routing.
- Fixed a problem where device would not boot if trying to connect to a port during boot time.
- Fixed a problem where telnet via IPv6 was disabled.
- Fixed a problem where HTTP redirection did not work using an IPv6 address.
- Fixed a problem where you couldn't set the date correctly.
- Fixed a problem where /var/log/wtmp was growing to large.

VERSION 1.1.5 April, 2008

- Fixed a problem where TCP/IP communication stops after receiving data over a PPP link running on the internal Modem.
- Fixed a problem where Dialin modem fails when using custom menus.

VERSION 1.1.4 December, 2007

- Added configurable option for local root access when setting remote auth for the CLI.
- Added support for remote authentication to the CLI without creating a local user.
- Added support for Spanish SAC.
- Added the ability to see suspicious intruders IP in system logs.
- Fixed a problem where SAMBA, NFS, and other settings can't be reset to defaults.
- Fixed a problem with Incorrect spacing in Portaccess Menu when port names are longer than expected.
- Fixed a problem with SAC support for the German language.
- Fixed a problem where the gateway was displayed incorrectly in the web ui if both ethernet interfaces have dhcp enabled.
- Fixed a problem where Clustering with master authentication fails if the user is > 19 characters.
- Fixed a problem where RSA SecurID - new Pin code and next token code mode did not work.
- Fixed a problem with user names greater than 30 characters Limited user name to 30 characters or less.
- Fixed a problem where the PC Card config is lost upon reboot.
- Fixed a problem where the system log time stamp was incorrect.
- Fixed a problem where Auto device detection fails to identify Cisco switch.

- Fixed a problem where PPP Option Allow client access to local network via PPP connection is not working.
- Fixed a problem where the wrong shell was being used when the CLI was configured for remote authentication.
- Fixed a problem where Clustering fails if any slave and/or peer has the Port access menu disabled.
- Fixed a problem where Access lists would fail when used in Peer to Peer config.
- Fixed a problem where Factory default does not default and backup the /usr2/rc.user file.
- Fixed a problem with NTP.
- Fixed a problem where SNMPv3 did not work correctly when configured for Auth/NoPriv.
- Fixed a problem where IP filtering for serial ports did not work correctly.
- Fixed a problem where you could not specify a range of serial ports for IP filtering.
- Fixed a problem where if a modem connection was dropped you could dial back in and not have to login.
- Fixed a problem where Fails auto uploading files via tftp to the /usr2 directory.

VERSION 1.1.3 April, 2007

- Added Rackable Management Card capability to Remote Ports.
- Enhanced user access controls for ports configured for a power controller.
- Changed "Start Device Locating" to "Activate Passport Locator LED".
- Added support for DRAC 4 and 5 on remote ports.
- Added support for iLO2 for Proliant servers on remote ports.
- Added support for SMASH CLP with DRAC 5 and iLO2.
- Enhanced Automatic detection.
- Added support for port groups.
- Fixed syntax error when unlocking a user account.
- Fixed a problem with IPMI SOL dropping connections.
- Removed all messages regarding KVM tool.
- Fixed a problem using the "more" command when connect via dial-in modem.
- Fixed a problem where SNMP was incorrectly reporting processor utilization.
- Fixed a problem where the Web UI became unresponsive.

Initial Release August, 2006