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 CM
Version 1.9.6 (November 12, 2019)

INTRODUCTION

This is the production release of firmware for the Digi CM. 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, and Memory cards, PCMCIA slot and configuration, custom menus, keyword monitoring and SMTP/SNMP notification, 10/100 mbps Ethernet network interface, and Digi Discovery server to allow discovery and network configuration from the Digi Discovery Applet.

SUPPORTED PRODUCTS

- Digi CM 48

KNOWN ISSUES

Important Note: With this release, because of space limitations on the device, the clustering function files have been removed from /bin and must be loaded manually to /usr2.

If you are updating from a previous version of CM firmware and you are using clustering, prior to upgrading to the new firmware you can issue the command # cp /bin/cl[us]* /usr2 to migrate the four necessary files to the new required location without having to upload them after the upgrade.

If you need to use the clustering functions, download the CM utilities file (80007071) from the digi web site and upload the clustering binaries to /usr2 following the instructions for adding clustering in the utilities file README.txt

KNOWN LIMITATIONS

- Web UI, Discovery Applet, and Serial Connection Applet require Netscape4.76 or higher or Internet Explorer 5 or higher.
- The Discovery Applet and Serial Connection Applet also require the Java Runtime Environment (JRE) 1.3 or higher.
- Netscape 4 on Windows: the serial port connection applet will not accept <enter> so the user cannot login through the applet.
- 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.

- Kerberos authentication has been removed. If you require Kerberos support, download the CM utilities file (80007071) from the digi web site. Copy kinit to the /usr2 dir on the Digi CM.
- If there are a large number of slave units configured the Master can take up to 8 minutes to boot up.
- The ftp client has been removed. If you require ftp support, download the CM utilities file (80007071) from the digi web site. Copy ftp to the /usr2 dir on the Digi CM.

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
1. 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
4. correctly installed)
5. Click on the "Basic" tab.
6. Verify "Enable Java Plug-In" is checked.
7. Click on the "Browser" tab.
8. Verify appropriate browser or browsers are checked.
9. Click on the "About" tab.
10. Verify Java Plug-in version is 1.3 or later.

When upgrading releases prior to 1.3.2, Digi advises you to factory default and reconfigure the CM after upgrading the firmware. If upgrading from rev. 1.3.2 or greater, importing configs will work with the exception of the “Serial port->User access control” section.

Digi CM firmware 1.7.0 or higher now uses the standard Digi Discovery Tool.
The original CM Discovery Tool will not work.
Revisions previous to 1.7.0 only supports the original CM Discovery Tool.

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, with the following exception:

- AnywhereUSB products manufactured before January 1, 2020, which currently do not have passwords set on them, will have a new default password of "dbps" after upgrading to this firmware. The respective username is "root". THIS NEW DEFAULT PASSWORD SHOULD BE CHANGED, this may be done via the web UI by navigating to Configuration – Security.

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 1.9.6 November 11, 2019

This is a mandatory release.

MD5 Checksum
69BCC515D27B5994F4044D45CA48A7E9 *cm48

SHA-256
ED5FF872255FE8E3ED40637855F1240FF4A099BD3BA054F8509FF087F05747A0 *cm48

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 1.95 May 10, 2010

- Added option to sync RTC with system time.
- Fixed a problem where The Web UI or Configmenu don't show the current Remote auth type for the CLI.
- Fixed a problem where Port locks up when accessing an Aix server via ssh and remote ports.
- Fixed a problem where Port access via web java app locks user account after only one failed login attempt.