Digi Passport FIPS
User's Guide Supplement

Digi Passport FIPS 4, Digi Passport FIPS 8,
Digi Passport FIPS 16, Digi Passport FIPS 32,
Digi Passport FIPS 48

November, 2009

90001126_A

Revision History

Revision	Date	Name	Description
A	Nov. 2009	SDA	Initial Release

Introduction

Due to the security restrictions inherent to a device operating in FIPS mode, some features of the Digi Passport are unavailable to the FIPS version of the Digi Passport. Similarly, some features/functions of the Digi Passport are changed or limited in the FIPS version of the Digi Passport. These changes are documented below in three sections: Special Considerations, Disabled Features, and Changed Features.

Special Considerations

The following are other important considerations for Digi Passports operating in FIPS mode:

Password Considerations

- The default user name is "**admin"** and the default password is "**dbpsfips**"
- New password rules:
  - Cannot include all of a user's account name (note that part of a user's account name is not checked)
  - Passwords must be between 8 and 255 characters long
  - Passwords must contain at least one of each of the following:
    - English uppercase characters(A-Z)
    - English lowercase characters(a-z)
    - Base 10 digits (0-9)
    - Non-alphabetic characters (!, $, #, %, and so on)
  - Six characters of a password may only occur once
  - No null or blank characters may be used
  - No consecutive numbers or letters

User Interfaces

- Firmware upgrade via the bios menu is not allowed.
  - Change the mode to NON-FIPS mode to upgrade firmware via bios menu.
  - Or, use the WebUI or configmenu to upgrade firmware while in FIPS mode.

Communication Protocols

- A different MIB is used from the regular Digi Passport due to some features being disabled in FIPS mode

Disabled Features

The following features/functions are disabled for Digi Passports operating in FIPS mode:

External Interfaces

- Locator LEDs
- PC Card
- Remote power controller
- Samba Server
- ServerTech network-enabled power strips
- USB: Expandable storage to USB

Communication Protocols

- Hash upgrade of individual files
- HTTP
- LDAP
- MD5 & DES
- Nonencrypted NFS
- Peer to Peer clustering
- Raw TCP
- Realport and encrypted Realport SMTP/Email
- SNMPv1/v2 get/set
- SSHv1
- SSLv1, v2, and v3
- Syslog
- Telnet

User Interfaces

- 192.168.1.100 port access
- 192.168.1.101 serial port address
- Configmenu scripting
- Direct Linux bash shell CLI access

Access/Authentication

- “root” user is not allowed to access the system
- NULL Password is not allowed in FIPS mode
- Master Authentication Mode
- Blowfish

Changed Features

The following features/functions are changed for Digi Passports operating in FIPS mode:

External Interfaces

- PC slot can be used until the Digi Passport is configured for FIPS mode

Communication Protocols

- ADDP is allowed in non-FIPS mode to initially discover the Passport on the network
- AES is allowed for privacy protocol.
- SHA is allowed for authentication protocol.
- SNMPv3 protocol is supported
- SSH protocol is supported
- TLSv1 is supported

User Interfaces

- “Zeroization” is added to the Configuration selection when attempting a factory default

Access/Authentication

- “Key Management” is a new menu which is used to manage all encryption keys in FIPS mode. This new menu includes:
  - Clustering encryption key
  - Configuration encryption key
- Clustering mode only supports local authentication