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

Digi One SP / Digi One IA Release Notes

Digi One SP / Digi One IA (82000774)

Revision Z (October 2020)

INTRODUCTION

This is a production release of firmware for the Digi One SP and Digi One IA. These devices provide high-performance serial port connectivity with added EIA-232/422/485 switch selectable support on the serial port. These devices come with RFC-2217 support, TCP Server (Reverse telnet/raw), Autoconnect (TCP Client), UDP Serial Client/Server, ARP-ping, Advanced Device Discovery Protocol, and Digi's patented RealPort protocol for COM port control.

SUPPORTED PRODUCTS

- Digi One SP
- Digi One SP Secure
- Digi One IA

KNOWN ISSUES

- Device performance may be affected if rpauth is enabled and the shared secret does not match the driver setting.
- Once a device is authenticated using RealPort Authentication it will stay authenticated for the duration of the RealPort session. If you change the rpauth state=disabled, you will need to reboot the device or restart the RealPort service. Simply closing the port does NOT stop the RealPort session.
- Due to system resource limits, connections to servers with an RSA key larger than 2048 bits are not possible.

UPDATE CONSIDERATIONS

- Before upgrading the 82000774 firmware, it is necessary that you have a POST firmware that supports the current revision of the 82000774 firmware. Failure to have a compatible POST will result in the device becoming unusable.

  To determine the current version of POST firmware using the WEB interface go

to the Administration/“Update Firmware” page. The “Update Firmware” page should display the current POST version and should look something like:

POST: release_82000775_F

To determine the current version of POST firmware using the command line interface, type “show versions” at the command prompt.

If the POST version is 82000775 revision A through E you must upgrade to the POST version 82000775_F or later.

If the POST version is 82001178 nothing needs to be done.

- This firmware version updates and restricts encryption to the device according to recent industry guidance and best practices. Given the resource constraints in this product architecture, and the increased computational power required to implement newer encryption methods, these latest changes may impact product performance in some applications, significantly increasing the time required for encrypted communications to complete. If application performance with this revision is not suitable, the best options are to revert to revision W firmware or use the product without using SSL/TLS encryption.
    - Connections are limited to TLS 1.2 to eliminate the possibility of downgrade attacks.
    - As a result of limiting the TLS protocol, if the customer wishes to use Encrypted Realport they will need to update to a version that supports TLS 1.2. Unencrypted RealPort is not impacted. Digi is in the process of updating the currently supported Encrypted RealPort drivers so this will become possible as those releases occur. Please refer to the RealPort driver page http://www.digi.com/support/realport/ for updates and information.
    - TLS services offer a public curve identity using a P-256 elliptic curve key. Clients must be capable of using ECC ciphers to connect.
    - The SSH implementation has been changed to use ECDSA keys. Previous DSA keys will no longer work and the key fingerprint/identity of the system will change after the update is applied. User accounts configured with public key identities will need to update these identities with new keys for SSH ‘publickey’ authentication to continue to work.
- On initial boot of this device, it will generate encryption key material. This process can take several minutes to complete. Until the corresponding key is generated, the device will be unable to initiate or accept that type of encrypted connection. It will also report itself as 100% busy but, since key generation takes place at a low priority, the device will still function normally. On subsequent reboots, the device will use its existing keys and will not need to generate another unless a reset to factory defaults is done, which will cause a new key to be generated on the next reboot.

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:
    1. Device firmware
    2. Configuration

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, knowledge base and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

82000774_Z (October 2020)

This is a recommended release

SECURITY FIXES

- CVE-2014-9223: A critical (CVSS 10.0) security buffer overflow in processing digest authentication has been fixed in the web server.

ENHANCEMENTS

- New TLS and SSH implementations put in place to modernize the security of the system. Details regarding functional changes impacting existing systems when upgrading from a previous revision are discussed in the UPDATE CONSIDERATIONS section above.
    - The TLS implementation offers a session cache for increased performance, particlarly when used with modern browsers.
    - New cipher suites and handshaking options have been added for increased security and performance.

*Release Notes Part Number: 93000459