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

Digi One IAP / Digi One IA RealPort Release Notes

Digi One IAP / Digi One IA RealPort (82000770)

Revision Z (October 2020)

INTRODUCTION

This is a maintenace release of the firmware (EOS) for the Digi One IAP and Digi One IA RealPort device servers. This product supports various intelligent protocol bridging including the new cross protocol bridging and Ethernet-to-Ethernet bridging. The hardware has isolated ground, DIN-rail mount, and transient surge protection.

SUPPORTED PRODUCTS

- Digi One IAP
- Digi One IAP Haz
- Digi One IA RealPort (renamed to Digi One IAP with Release “E”)

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.
- (Relevant ONLY during protocol converstion) PLC5 Typed Rd/Wr and Word Range Rd/Wr are optimized to mimic behavior of ControlLogix, SLC5/05 and MicroLogix 1200 when handling these commands. This means PLC5 as target (slave) should always work, however PLC5 as originator (master) may attempt address combinations that are not understood and could result in unpredictable Modbus responses.
- Rockwell users who want to use RSLinx and RSLogix to access serial PLC must enable at least the AB/Ethernet (CSPv4) Net Master; they cannot access solely by Ethernet/IP. This is a limitation in how RSI implements its tools, not the Digi

firmware! With only Ethernet/IP active, RSI tools will attempt to issue unsupported PCCC commands which results in a diagnostic failure.

- MicroLogix 1000 PLC do not work with some RSLinx versions due to RSLinx sending unsupported Diagnostic Queries to “IP-based” PLC which are too advanced for the MicroLogix 1000

UPDATE CONSIDERATIONS

- 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.

UNDERSTANDING YOUR HARDWARE

Two hardware boards exist; the easiest way to absolutely determine which board you have is by examining the Web Interface “Update Firmware” page. The POST file (like a BIOS) defines which hardware you have.

A POST file such as 82000779_D indicates the older board made until spring 2007. Another way to tell is examine the Ethernet Link LED - on this board it is RED with no cable attached and dark with GoodLink. These boards can run firmware D, D1, E, E1, F and G.

WARNING: “G” firmware requires POST 82000779_D or higher on older boards Users of firmware “D/D1” *MUST* upgrade their POST FIRST! Users of firmware “E/E1/F/G” already have the correct POST installed.

A POST file such as 82001178_F indicates the newer board made starting spring 2007. Another way to tell is examine the Ethernet Link LED - on this board it is dark with no cable attached and GREEN with GoodLink. These boards MUST run firmware G and cannot be back rev'd. The hardware has changed to the point older firmware would not understand the board.

The POST files 82000779_D and 82001178_F *CANNOT* be swapped; 82000779_D cannot be upgraded to 82001178_F since the POST must match the hardware.

ADDITIONAL INFORMATION

Switching between 1 and 2 ports

Newer Digi One IAP hardware has a dip-switch that allows switching between 1 and 2 port modes. In 2-port-mode the screw terminal connector is port 1 and the DB9 connector is port 2.

It is necessary that the device be power cycled after switching between 1 and 2 port modes. Failure to do so will result in unpredictable device behavior.

If you are using Digi's RealPort technology (allows the device's serial ports to appear as if they were on the local computer) it is highly recommended that you reconfigure or reinstall the RealPort driver after switching between 1 and 2 port modes. Failure to do so may result in RealPort not functioning correctly.

POST & FIRMWARE UPDATE

You can update the POST and/or firmware of your device server either through the device server's web interface or command line interface.

NOTE: When updating the firmware of your device server to a new version, please ensure that you are running the most recent POST as well. If you need to update your POST, it must be done BEFORE the firmware update.

Please ensure that you are running POST 82000779_D or higher.

POST update via the web interface

Log on to the device server's web interface. Go to Administration > Update Firmware. In the From a File section, select POST from the Update list. Click Browse... and navigate to the POST file. Click Open, then click Update.

When the update process has finished, click Reboot to restart the device server.

POST update via the command line interface

This option requires a TFTP server. First, copy the POST image to the TFTP server. Then, log on to the device server's command line interface and update the POST with the following command:

```
boot load-boot=<IP address of TFTP server>:82000779_D.bin
```

When the update process has finished, restart the device server with the following command:

```
boot action=reset
```

Firmware update via the web interface

Log on to the device server's web interface. Go to Administration > Update Firmware.

In the From a File section, select Firmware from the Update list. Click Browse… and navigate to the firmware file. Click Open, then click Update.

When the update process has finished, click Reboot to restart the device server.

Firmware update via the command line unterface

This option requires a TFTP server. First, copy the firmware image to the TFTP server. Then, log on to the device server's command line interface and update the firmware with the following command:

```
boot load=<IP address of TFTP server>:82000770_E.bin
```

When the update process has finished, restart the device server with the following command:

```
boot action=reset
```

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

82000770_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: 93000464