SNIB3 2.03.1008 Firmware Release Notes

Overview

This document describes the new features and enhancements of the Secure Network Interface Board v3 (SNIB3) firmware, compared to the 2.02.0026 release of the SNIB3 firmware. This document also summarizes the Bug Fixes and the Known Limitations in this 2.03.1008 release of the SNIB3 firmware.

The versions of the SNIB3's firmware components in this release are:

Firmware:	**02.03.1008**
OS:	**01.04.0002** (01.05.0000 is used for the Mx-1 controller's built-in SNIB3 capability**)**
Driver:	**01.05.0002**

The required versions of associated programs to support this release of the SNIB3 firmware are:

Velocity:	**3.7** (build 03.06.008.1483)
CCM:	**7.6.20.25**

If the SNIB3 is on the same network subnet as the Velocity host, then you will configure it using Velocity. If the SNIB3 is on a different subnet, then you will begin to configure it using the SNIB Configuration Tool. While trying to discover SNIB3s, you should temporarily disable port monitoring tools (such as Norton Antivirus and Windows firewall) or add **Velocity.exe** and **SNIBConfigTool.exe** to the exceptions list.

Upgrading the firmware of downstream SNIB3s must be done one at a time. In a master-slave configuration, you must upgrade the master SNIB3 board's firmware first, and then upgrade each slave SNIB3 board's firmware in sequence. Don't start the download for the next SNIB3 board until the firmware upgrade for the previous SNIB3 board has completed.

Information about installing and configuring the SNIB3 is provided in the **SNIB3 Quick Installation Guide** which is included with each order. Complete information about the SNIB3 is included in recent versions of the **DIGI*TRAC Systems Design and Installation Guide** (dated 9/20/2016 or later).

NOTE: The SNIB3 can also be used in an Mx-4, Mx-8, or M64 controller which is part of an Identiv Connected Physical Access Manager (ICPAM) version 3.0 or later system. Build 2.01.0025 or later of the SNIB3 firmware is required for the ICPAM 3.0.1 release, which provides support for URL trigger actions for Mx-4, Mx-8, and M64N controllers.

The functionality of the SNIB3 is built into the main board of the single-door Mx-1 controller (instead of requiring an expansion board).

The minimum required versions of associated programs to support the SNIB3 as part of Identiv's FICAM Solution are:

Velocity:	**3.6 SP2** (or later)
CCM:	**7.5.64.95** (or later)

For most customers, Identiv's FICAM Solution enables you to upgrade an existing Velocity system, instead of having to purchase and install a new physical access control system. Even when FICAM mode is enabled, the other components of your existing Velocity system will continue to function as before. This enables a smooth migration as you replace old readers and enroll new credentials.

For more information, see the **FICAM Solution** section of topics in the Velocity main help system. Information about the hardware components (including the SNIB3 and the RREB) is provided in recent versions of the **DIGI*TRAC Systems Design and Installation Guide** (dated 1/27/2017 or later).

New Features and Enhancements in this Release

This SNIB3 2.03.1008 firmware release provides support for Assa-Abloy's Aperio wireless locks. (For information about this feature, see the **Velocity 3.7 Release Notes** and the new "DIGI*TRAC Hardware Configuration > **Wireless Locks**" section in the **Velocity 3.7 main help**.)

Bug Fixes

"Card reader LED on while relay active" option was not working properly (PAC-683)

When the **Card reader LED on while relay active** option (on the **Options** page of a **Reader Properties** dialog) was checked, the LED was turning on with the door relay after the first access grant, but it was not turning off after the door relay closed. This issue has been fixed.

Known Limitations

Recommended Baud Rate for master/slave communication is 9600

For RS-485 serial connections between a master SNIB3 and downstream SNIB2s or SNIB3s, the SNIB3 works best when the baud rate is set to 9600 bps.

Simultaneous downloads of many credentials can cause the downloads to hang

Occasionally, the simultaneous download of a large number of credentials to a master SNIB3's controller and all of its downstream controllers can cause the downloads to hang. When this occurs, you must either disconnect and reconnect the master SNIB3's network cable or reboot the master SNIB3's controller, after which the download will continue where it left off. We recommend downloading credentials to one controller at a time.

Simultaneous Firmware Download of slave controllers results in firmware download error (FAL-724)

When attempting to download firmware updates simultaneously on two or more downstream SNIB3-attached controllers, a firmware download error will occur. This is a previously documented limitation that occurs in both SNIB2- and SNIB3-attached controllers.

Workaround: It is recommended and standard practice to only download firmware to one controller at a time on a given port. Attempting to download firmware updates to more than one controller at a time will result in firmware download errors.

When changing from XNET2 to XNET3 mode, controllers are logged off, but port shutdown does not happen (FAL-729)

If you attempt to change the mode of downstream controllers from XNET2 to XNET3 protocol, the controllers log off but a proper port shutdown does not occur.

Workaround: The port has to be disabled before changing protocols.

State-full IPv6 addresses are not supported (FAL-772)

Because state-full IPv6 addresses are not currently supported, if your network uses only state-full IPv6 addresses, a SNIB3 will not be discoverable. (A SNIB3 will be discovered if it is using static IPv6 addressing, stateless IPv6 DHCP addressing, or IPv4 addressing.)

After starting up and synchronizing with the CCM, there is a 5-second delay before the SNIB3's LEDs display normal patterns (FAL-846)

After a controller is powered on, its SNIB2 or SNIB3 board displays a circular pattern on its LEDs while synchronizing with the CCM. Then various other patterns are displayed during normal operations. But with the SNIB3, there is a 5-second delay after synchronization before the LEDs start displaying the patterns for normal operations.

While performing a download of a CCM firmware update to a standalone controller, its Port and XBOX go offline and come back online (FAL-949)

While performing a download of a CCM firmware update to a standalone controller, its Port and XBOX go offline and come back online. (This issue does not happen for a controller which is the Master in a chain of connected controllers.)

Disconnecting the Ethernet cable from a master SNIB3 for a long period of time generates spurious online/offline messages for the RS-485 TS readers connected via an RREB to that SNIB3 (FAL-982)

Disconnecting the Ethernet cable from the master SNIB3 in a chain of connected controllers for a long period of time generates spurious online/offline messages for the RS-485 TS readers connected via an RREB to that SNIB3. Downstream SNIB3s in the chain are not affected.

For example, if the Ethernet cable is disconnected from the master SNIB3 for a period of 24 hours, after the Ethernet cable is reconnected all of the RS-485 TS readers connected via an RREB to that SNIB3 will report “Reader X Offline” and “Reader X Online” messages in Velocity’s Event Viewer.

RS-485 readers which are configured in Velocity but are not physically connected sometimes report as secure (FAL-988)

When RS-485 readers are configured in Velocity but are not physically connected to an RS-485 port of the RREB in a controller running in FICAM mode, they sometimes report as secure when powering up the controller.

Unexpected colors displayed when multiple options are selected

The Options page of the reader properties dialog in Velocity has many options. The options in the Scramblepad/Keypad category include **Green LED always on**, **Red LED always on**, and **Yellow left LED always on**. If you select more than one of these options, the color displayed by the reader may not match your expectations.

Enable Scramblepad Sharing option is not implemented

The **Enable Scramblepad Sharing** option (in the Card Reader category on the Options page of the reader properties dialog in Velocity) is not implemented in this release.

Non-FICAM cards are not read by TS readers (in a specific situation)

For a reader with the **RS-485 Interface**, the Logic page of the reader properties dialog in Velocity includes the ability to specify both a **default assurance level**, and a **lower assurance level** during certain time periods (such as when a security guard is on duty). The choices available for these assurance levels depends on the specific reader type, and if a lower assurance level is specified it will only be used when a time zone is also selected to activate the CCOTZ feature. (For more information about these features, see the **Velocity 3.6 SP3 Release Notes**.)

For a Reader Type of **TS**, **TS-Scramblepad**, or **TS-Keypad**, non-FICAM cards are not read in CCOTZ mode, if the “Default assurance level” option is set to the **CAK/Card** value and the “Enable lower assurance levels” option is unchecked.

Workaround: Make sure that the “Enable lower assurance levels” option is checked in this situation.

When an Aperio AH30 communication hub is reset, it loses the status of its paired wireless locks (PAC-619)

During normal operation, when an Aperio wireless lock comes online, if it is in a lock tamper state, that information will be reported to Velocity. But when an Aperio AH30 communication hub is reset, it loses the status of its paired wireless locks. So if the hub is reset and then a wireless lock goes offline and comes back online, its tamper state might not be reported to Velocity.

When an Aperio wireless lock goes offline, Velocity does not display the correct alarm message (PAC-726)

When an Aperio wireless lock goes offline (such as when its batteries are removed), Velocity displays a generic event message of “Device offline at Door X” (instead of the specific alarm message “Wireless Reader at address Reader X offline”). Similarly, when an Aperio wireless lock comes back online, Velocity displays a generic event message of “Device online at Door X” (instead of the specific alarm message “Wireless Reader at address Reader X online”).

If an Aperio AH30 communication hub's wireless lock position 1 is not configured, “hub restarted” events are not displayed in Velocity (PAC-834)

During normal operation, when an Aperio AH30 communication hub is reset, it reboots and “hub restarted” events are displayed in Velocity. But if the hub’s wireless lock position 1 is not configured, then those events are not displayed in Velocity. (This issue occurs because the hub shares the same address as the wireless lock at position 1, so when position 1 is not configured, the SNIB3 cannot poll the hub to obtain its events.)