# SNIB3 2.01.0011 Firmware Release Notes



## Overview

This document describes the new features and enhancements of the Secure Network Interface Board v3 (SNIB3) firmware, compared to the 1.07 release of the SNIB3 firmware. This document also summarizes the Known Limitations in this 2.01.0011 release of the SNIB3 firmware.

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

| | |
|---|---|
| Firmware: | **02.01.0011** |
| OS: | **01.04.0002** |
| Driver: | **01.05.0002** |

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

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

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 or Mx-8 controller which is part of an Identiv Connected Physical Access Manager (ICPAM) version 3.0 or later system.

## New Features and Enhancements in this Release

The SNIB3 is a major hardware component of Identiv's FICAM Solution, and this SNIB3 2.01.0011 firmware release provides the following new features:

- support for Identiv's uTrust TS Government readers (which are FICAM-capable RS-485 card readers)
- support for FICAM Card Challenge by Identiv's uTrust TS Government readers
- support for Card Authentication Key (CAK) certificate validation for access requests
- support for FICAM Degraded Mode, where the behavior can be specified for each reader
- support for PACS PIN + FICAM Card
- FIPS 140-2 certified cryptography

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

| | |
|---|---|
| Velocity: | **3.6 SP2** |
| CCM: | **7.5.64.95** |

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 the latest version of the **DIGI*TRAC Systems Design and Installation Guide** (dated 1/27/2017).

# Known Limitations

### SNIB3 supports only 16 downstream controllers

Although the SNIB3 (like the SNIB2) is intended to support up to 63 downstream controllers when using NET*MUX4s, this feature is not yet implemented. In this release, a SNIB3 can support up to 16 downstream controllers.

### 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 problem 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.

### Function Groups do not work when a TS ScramblePad is connected to an RS-485 port of the RREB in a controller running in FICAM mode (FAL-986)

When a TS reader with a keypad is connected using the Wiegand protocol, it operates in **burst mode** which transfers all of the key presses (including the asterisk key) “as is” to the controller. But when a TS ScramblePad is connected to an RS-485 port of the RREB in a controller running in FICAM mode, it operates in a **buffered mode** where pressing the asterisk key clears the buffer contents so the asterisk and the numbers entered before it are not sent to the controller. This means that you cannot use function groups or perform keypad programming.

### 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.