How to replace a firmware chip on a Lenel Intelligent System Controller

Last Modified on 10/06/2022 4:19 am EDT

How to replace a firmware chip on a Lenel Intelligent System Controller

Procedure Steps

Important:

- When replacing any firmware chip, follow standard electrostatic discharge guidelines to avoid damage to the Intelligent System Controller (ISC).
- Use a chip puller to remove the firmware chip to avoid damaging the firmware chip and/or the ISC board.

1. Remove power from the ISC.
2. Place a non-metallic object, like an access card, between the coin cell battery contact and battery.
3. Using a chip puller, remove the old firmware chip (32-pin DIP with the white paper label) from the ISC.
4. Note the orientation of the firmware chip. Install the new firmware chip on the ISC with the proper orientation, taking care not to bend the pins of the chip.

-
    - Each chip has a little indentation at one end of the chip. The ISC board has a box around the location where the chip is installed and one end has a notch; the indentation needs to line up with this notch.
    - When installing the new chip, gently seat the new chip and ensure that all the pins are aligned in the proper location before pressing down on the chip. Press down evenly to avoid bending any of the pins.

5. Remove the non-metallic object from between the coin cell battery contact and battery.
6. Apply power to the ISC.
7. Once the ISC shows an online status in Alarm Monitoring, perform a database download to the ISC.

Applies To

LNL-500 Intelligent System Controller
LNL-1000 Intelligent System Controller
LNL-2000 Intelligent System Controller

Additional Information

How to determine whether a firmware chip needs to be replaced

There is no way to determine the version of firmware on the chip by looking at the chip. If you download the firmware and are unable to update to the newer firmware, then you must follow this process to replace the firmware chip on the ISC.

Impact of replacing the firmware chip

When replacing the firmware chip, all functions controlled by the ISC will be impacted, such as (but not limited to) the following:

1. The ISC will be offline when it is powered down. While the ISC is offline:

-
    - Readers will revert to offline mode
    - Local I/O will stop
    - Global I/O will stop
    - Anti-passback enforcement will cease
    - Panel-based biometrics will cease
    - Events will not be stored and will be permanently lost (events will not be buffered on the I/O panels)
    - Device-camera links will cease to function

2. Once power is restored, a database download will be required for each ISC.
3. After a download, realtime state information will be reset, including but not limited to the following:

-
    - Reader modes will revert to their default online state, so if timezone reader modes are active then you may need to manually set some readers to the desired mode.
    - Anti-passback locations may be reset if local anti-passback is active.