Lantronix, Inc.
12755 Highway 55, Ste H100
Plymouth, MN 55441
www.lantronix.com

ION x323x Release Notes
Date: November 6, 2026
Version: v1.3.36/37

Overview
This release note covers the requirements, important notes, new features and changes, addressed issues and known limitations for the ION x323x products.

Management of the ION x323x is available using a web browser, SNMP or one of the Command Line Interfaces (CLI) - the local USB port, telnet or ssh.

Firmware v1.3.36/37 and these release notes apply to the following products:

- C3230-1040 and C3231-1040
- S3230-1040 and S3231-1040

New behavior – Enforced 'ION' admin user password change from default password, 'private':
Before upgrading – if the upgrade target has been configured to local management mode ('set switch mode local' was previously run on the CLI), the 'ION' admin user account will force a password change using the CLI on first login of the new firmware whenever the password is the default – 'private'. Changing the password prior to upgrade will allow you to use the WebUI or the CLI to set the password. After the upgrade, the CLI will need to be used.

Please note that new units are shipped with management mode set to remote – the enforced password change is only for local management mode. Units in a managed chassis (with an IONMM) are very likely left in the default remote management mode and unaffected by the new password policy.

On a factory-reset, units will be reset to remote managed mode – setting the management mode to local will require the password change on the CLI.

New behavior – Secure services enabled by default after factory reset and on new shipped units
Once local management is enabled, the new services are:

- SSH is enabled
- Telnet is disabled
- SNMP is disabled
- HTTPS + HTTP redirect is enabled

IMPORTANT UPGRADE INSTRUCTIONS WHEN STARTING FROM FIRMWARE v1.3.26 AND OLDER:

- **Install firmware v1.3.36**
- **Wait for ION x323x to boot**
- **Re-boot ION x323x**
- **Install firmware v1.3.37**
- **Installing v1.3.37 or any future release will refresh the NAND**
- **If needed, once v1.3.37+ has been installed, user can downgrade to previous firmware versions. However, if running versions prior to v1.3.37, it is recommended to repeat refresh process (v1.3.36, reboot, v1.3.37+) at least once every 3 years to keep NAND refreshed. Ignoring the refresh process for too long will result in an ION x323x that will not boot.**

New Features and Enhancements:

The following enhancements are incorporated into firmware v1.3.36/37:

- NAND refresh
- HTTP-to-HTTPS re-direct when HTTPS is enabled
- Disabled deprecated TLS 1.0/1.1 – TLS 1.2 is used for https operation
- Added SFTP support

Security Updates:

Remote SNMPv1/v2c access is disabled until explicitly enabled

Firmwares 1.3.26 and prior, the agent answered remote SNMPv1/v2c out of the box with the documented default communities `public` (read-only) and `private` (read-write).
After upgreading to 1.3.36+, remote SNMPv1/v2c polling and SETs no longer respond (the access state fails closed when upgrading from older firmware). This is the most visible change of the release: any management system polling the unit with `public` will stop receiving data.
To re-enable, from the CLI, run `set snmp state=enable` (a reboot is required; the CLI prints a reminder), then optionally set custom communities with `set community read=<ro> write=<rw>`. These SNMP v1/v2c management commands — `show snmp config`, `set snmp state`, `set community` — are new in this release.
When enabled with default communities, `public` (read-only) and `private` (read-write) work as before. Setting custom communities replaces the defaults; once custom communities are configured, the default strings are rejected. Setting custom communities — particularly a custom read-write community — is strongly recommended, since the defaults are published in the documentation and SNMPv1/v2c traffic is sent in the clear.
SNMPv3 is unaffected: existing SNMPv3 users continue to work, and user creation/management is unchanged.
Trap delivery is unaffected.

SNMP management tables are never exposed to remote walks

Whenever remote SNMPv1/v2c access is enabled, the external communities are granted a restricted view that excludes the SNMP configuration MIBs: the community table (community strings), the view-based access control (VACM) tables, and the SNMPv3 user (USM) table. This closes a serious exposure in

earlier releases, where an unauthenticated walk with the read-only community disclosed the read-write community string and the complete access policy. This restriction is unconditional — it applies to all remote communities, read and write, and cannot be configured away. (When walking the excluded subtrees, the agent returns an end-of-view message — "No more variables left in this MIB View" — rather than data; this is the restriction working as intended, not an error condition.)

Account passwords are stored hashed
Existing passwords continue to work after upgrade. The next time a password is set (by any interface), it is stored as a one-way crypt() hash instead of recoverable text. Backup/restore carries the stored (hashed) form without changing it. Password and user-name fields are now restricted to printable, non-whitespace characters. Any account created on earlier firmware with spaces in its password should be re-created or re-set after upgrading (contact support if login fails).

HTTPS redirect and web headers
On units with HTTPS enabled, plain-HTTP connections on port 80 are now redirected (HTTP 301) to HTTPS, preserving path and query. Previously both ports served content independently. Units that have not enabled HTTPS are unaffected.
HTTPS responses now include HSTS; all web responses include `X-Frame-Options: SAMEORIGIN` (blocks framing/clickjacking).
New units and factory-reset units have HTTPS enabled by default with a self-signed `lantronix.com` certificate (installable/replaceable via the WebUI HTTPS page)

SSH and telnet are independent services
Enabling SSH no longer stops the telnet service, and each service has its own enable/disable setting.
Telnet can now be enabled/disabled from the CLI (`show telnet config`, `set telnet server state=...`) and from the WebUI.
Upgraded units keep their current service state.
On **remotely managed** units, neither the SSH nor the telnet daemon runs; management access is via the managing unit, or the local console (`set switch mode local` from the console switches the unit to local management mode, which starts the SSH daemon after a reboot).

WebUI session and privilege enforcement
Web sessions use unpredictable random session IDs; sessions expire after 24 idle hours and do not survive a reboot.
Authorization is now enforced by the device, not only by the web client: read-only users can no longer perform configuration changes directly through the web interface, and user-table modifications require an admin session.
WebUI sessions now survive SNTP clock steps and manual time changes (previously such steps could end sessions).

CLI hardening
The CLI has removed shell-injection opportunities (CVE-2026-18530).

To configure the new secure default services without a factory reset:
From the a3cli, run these commands:

```
set ssh server state=enable
set https state=enable
set telnet server state=disable
set snmp state=disable
reboot
```

These commands put the unit in the new service state without affecting other settings (IP, tftp, users, trap server, etc…).

Downgrading
It is not recommended to downgrade as the security fixes in 1.3.36/37 are necessary to keep the devices secure. If you need to downgrade, follow these guidelines.

Downgrading new ION media converters
New units come in remote management mode and should be downgraded in this mode. If local management mode is set, the ION user will be forced to change their password before anything else can be done and the hashed passwords in 1.3.36/37 are not compatible with earlier releases.

For chassis cards, put them in a chassis with an IONMM and downgrade them to the desired release.

For stand-alones. connect them as a remote to an existing chassis/stand-alone and use the management node to downgrade to the desired release.

As long as the downgrade happens with the unit in remote management mode, the unit will behave exactly as though it came with the downgraded release from the factory. If it is subsequently set to local management mode, it will use HTTP and telnet.

Downgrading existing ION media converters after completing the NAND refresh
If you need to keep your unit at the version it is at currently, the NAND refresh still needs to happen.

Before upgrading to 1.3.36, units in local management mode need to have their password set for the ION user to something other than ‘private’. Failure to do so will force a password change once at 1.3.36 that is incompatible with previous releases.

Units in remote management mode do not need to have their password changed as long as they are left in remote management mode throughout the upgrade/downgrade process.

To accomplish a NAND refresh, install 1.3.36 and let it boot. Once it is booted, reboot it, After the reboot, install 1.3.37 and let it boot. At this point the NAND is refreshed and the unit can be downgraded to the desired release.

Related Documentation:

- ION x222x & x32xx User Guide (33472)
- ION x222x & x32xx Installation Guide (33433)
- ION Command Line Interface Reference Guide (33461)

Known Limitations:

- Stand-alone with attached remote, attempting to reboot the remote will reboot the local (stand-alone) unit
- Fiber intrusion trap is not generated when threshold is cross
- Trap message is not sent when Remote loses fiber connection
- Editing stand-alone stack name will also reflect the change in Local device
- Full port/service scanner probes aimed at the unit's management LAN address can cause temporary unit unresponsiveness – management recovers after a reboot.
- Trap host display after upgrade:** trap destinations configured on earlier releases keep delivering traps after the upgrade, but the trap host list shown by `show snmp config` (and the corresponding WebUI display) may show unset entries or a retrieval message until the destination is re-entered. Delivery is unaffected; if you do re-enter the destination, confirm your collector is not receiving duplicate traps.

MIBs

- ion_mibs-2026.11