California Senate Bill 327 – Required Changes for PDU Compliance

This technical note provides information about the new California law, **Senate Bill 327**, as follows:

- Highlights what you can expect from this Bill in 2020 in our PDU products and firmware;
- Informs you of Server Technology's action plan and implementation strategy for compliance;
- Tells you what to do if you perform automated or bulk configuration/provisioning of new PDUs.

What Is This Bill?

In September 2018, California Governor Jerry Brown signed a cybersecurity law, **Senate Bill 327**, covering Internet of Things (IoT) devices to incorporate minimum security features for every device, making California the first state with such a law.

Starting January 1, 2020, the bill, **SB-327,** requires any manufacturer of a device that connects "directly or indirectly" to the internet to be more responsible for ensuring privacy and security for California residents by equipping devices with "reasonable" security features that are designed to prevent unauthorized access, modification, or information disclosure.

If the device can be accessed outside a local area network with a password:

- The device needs either to come with a unique password for each device, or
- The device must force users to set their own password the first time they connect, eliminating generic default credentials that could be hacked. **Note:** This is the route Server Technology has chosen to implement.

A "connected device" is defined as a device with an Internet Protocol (IP) or Bluetooth address, and capable of connecting directly or indirectly to the Internet.

The **SB-327** bill, and related bills, are designed to protect devices and their information from "unauthorized access, destruction, use, modification, or disclosure." Note that there may be other similar bills in the near future originating in other states, or nationally. If so, Server Technology will keep you informed in updated Technical Notes.

Server Technology's Action Plan

To comply with **SB-327**, for Server Technology's PROx PDU products, and for the PDU's firmware, the following plan has been implemented by Server Technology, starting with firmware version 8.0q for January 2020.

What's new in firmware version 8.0q:

- Factory-default changes:
  - Only secure access (physical or by secure network protocols) is enabled by default.
  - **Before logging in**, you are forced to change the default password.
- Configuration changes to enable insecure features provide a warning, require confirmation, and are logged.

Default PDU configuration:

The factory default configuration has these services changed to **disabled**:

- Telnet Server
- SNMP Agent
- HTTP Server
- FTP Server
- STEye (Server Technology's Bluetooth interface for mobile applications)
- SNAP (protocol for Sentry Power Manager [SPM] software)

The factory default configuration has these services remain **enabled**:

- HTTPS Server
- SFTP Server
- SSH Server
- Console
- SUS (StartUp Stick USB/I2C bulk configuration tool)
- ZTP (Zero Touch Provisioning)

Notes:

- Firmware updates to units in the field do not change any defaults until a reset to factory defaults occurs.
- The network TCP/IP stack, DHCP, LLDP, and SNTP remain enabled by default.

Default password change requirement:

The default password must be changed upon first use, before any other configuration changes or device access are allowed. In factory default configuration, the following protocols and tools, with the following restrictions, allow you to first update the default password:

HTTPS Server Web User Interface:

- Restricted to a password change page/form only

HTTPS Server JAWS (JSON API Web Service):

- API limited to only system identification and a password change for the default account

SSH Server:

- Prompts for a password change

Console:

- Prompts for a password change

SFTP Server:

- Restricted to write-only of a Server Technology INI Configuration (STIC) file
- STIC configuration changes will only be applied if they include a default password change

Start Up Stick (SUS):

- STIC configuration changes will only be applied if they include a default password change.

Zero-Touch Provisioning (ZTP):

- STIC configuration changes will only be applied if they include a default password change.

Notes:

- Once the default password is changed, the restrictions are removed and the PDU resumes normal operations for the protocols and tools listed above.
- Upon any restart to factory defaults, the restrictions will again be enforced and a change to the default password will again be required.

PDU Automated Configuration, Bulk Configuration, and Provisioning

PDU automated configuration, bulk configuration, and provision processes are still supported by firmware version 8.0q PDUs in factory default configuration, although with restrictions and changes:

- If you are using your own automation and configuration tools to provision PDUs, you will have to accommodate the required changing of the password the first time you access the PDU. You also may need to change to an enabled protocol, for example, to SSH from Telnet.

- If you are performing configuration or provisioning by loading a STIC text INI file (via SFTP, ZTP, or SUS), the changes must include a default password change; otherwise, no changes will be applied.

Contact Technical Support

be supported.

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product.
Free Technical Support is provided from 8 a.m. to 5 p.m. Pacific Time, Monday through Friday.

Server Technology, Inc. (a brand of Legrand)

1040 Sandhill Road Tel: 1-800-835-1515 Web: www.servertech.com
Reno, Nevada 89521 USA Fax: 775-284-2065 Email: support@servertech.com

stay powered. be supported. get ahead.

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.