
Liebert® IntelliSlot™ RDU101 Card

Version 1.0.0.3_0000005 Firmware

Release Notes

February 11th, 2019

This document outlines:

1. Version and Compatibility Information
2. What's New
3. Security Issues Addressed

1. Version and Compatibility

This release contains the following firmware version:

RDU101

This release is compatible with the following Liebert IntelliSlot communication cards:

RDU101

This release is compatible with the following power and thermal management equipment:

Liebert GXT5™

This release is compatible with the following sensors:

Liebert SN-T	Liebert SN-Z01
Liebert SN-TH	Liebert SN-Z02
Liebert SN-2D	Liebert SN-Z03
Liebert SN-3C	

This release supports the following features:

Communication Card	LIFE™ Services Support	Sensor Support	Communication Protocol							
			HTTP/HTTPS	Velocity Protocol	Email	SMS	Third-Party Protocols			
							SNMP v1,v2c,v3	BACnet IP/MSTP	Modbus TCP/RTU	YDN23
RDU101	✓	✓	✓	✓	✓	✓	✓	-	-	-
Sensor Support			✓	✓	✓	✓	✓	-	-	-

This release supports the following browsers:

- Microsoft Internet Explorer®
 - IE10 - 10.0.9200.17457
 - IE11 - 11.0.9600.18837
 - Edge - 42.17134
- Mozilla Firefox® - ver. 59.02
- Google Chrome™ - ver. 69.0.3497

2. What's New

This release contains the following enhancements:

- The web bezel (power flow diagram) was enhanced to provide a more accurate UPS status.
Example: Battery charging in addition to Battery discharging is now available.

3. Security Issues Addressed

The following highly publicized security vulnerabilities have already been addressed in this release:

Name	Description
"ShellShock"	The appropriate version of bash is implemented
"Poodle"	SSLv3 is disabled
Cross-Scripting	Cross-Scripting entries via the Web user Interface are restricted
"Clickjacking"	Clickjacking is addressed in this release.
"Beast" and "Logjam"	The "Beast" and "Logjam" vulnerabilities are addressed
TLS 1.0 access	TLS 1.0 is disabled so only newer versions are used.
"Sweet 32 Birthday Attack"	Vulnerability Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) is addressed.

4. Issues Addresses

Component	Description
Web – Active Networking page	The Active Networking Web page was indicating incorrect information. This issue has been resolved.

5. Known Issues

Component	Description
None	