
Liebert® IntelliSlot™ Unity Card

Version 7.8.0.0_00083 Firmware

Release Notes Rev 1

January 21st, 2020

This document outlines:

1. Version and Compatibility Information
2. What's New
3. Security Issues Addressed
4. Upgrade Instructions
5. Known Issues

1. Version and Compatibility

This release contains the following firmware version:

IS-UNITY_7.8.0.0_00083

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

IS-UNITY-DP, IS-UNITY-SNMP, IS-UNITY-LIFE

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

Alber BDSU-50	Liebert HPM
Liebert APM	Liebert ITA2/EXS
Liebert APS	Liebert Mini-Mate
Liebert CRV	Liebert NX 225-600kVA
Liebert CW*	Liebert NXC
Liebert Challenger*	Liebert NXL
Liebert Deluxe System/3*	Liebert NXR
Liebert DCL	Liebert PCW
Liebert DCP	Liebert PDX
Liebert DP400	Liebert PeX*
Liebert DS*	Liebert PPC
Liebert DSE	Liebert PSI5
Liebert EPM	Vertiv™ Edge
Liebert EXC	Liebert RDC
Liebert eXL	Liebert RX
Liebert EXL S1	Liebert STS2
Liebert eXM	Liebert XDC with iCOM™ Control
Liebert FDC	Liebert XDP with iCOM™ Control
Liebert FPC	Liebert XDP-Cray
Liebert GXE2	Liebert XDU
Liebert GXT3 / GXT4	
Liebert HPC-S,M,R,W,Generic	

*iCOM Firmware PA1.04.033.STD versions or later

This release is compatible with the following sensors:

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

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
IS-UNITY-DP	✓	✓	✓	✓	✓	✓	✓	✓	✓	NXL, EXL S1 & PeX
IS-UNITY-LIFE	✓	✓	✓	✓	✓	✓	-	-	-	-
IS-UNITY-SNMP	✓	-	✓	✓	✓	✓	✓	-	-	-
Sensor Support			✓	✓	✓	✓	✓	-	-	-

This release supports the following browsers:

- Microsoft Internet Explorer® - IE10, IE11, Edge
- Mozilla Firefox® - ver. 71.0.1 or later
- Google Chrome™ – ver. 72.0.3 or later
- Safari® (MacBook®) - ver. 8.0.5
- Safari® (iPad®) - ver. 7.1

2. What's New

This release contains the following enhancements, updates and corrections:

- Vertiv Edge *initial release*
- CRV10/PACC
- EXL
- iCOM PA XDU
- EXS Frame 2/3
- Compliance with California IoT Law

3. Security Issues Addressed

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

Name	Description
"ShellShock"	Updated bash version to fix this in release 4.2
"Poodle"	SSLv3 was disabled in release 5.0
Cross-Scripting	Cross-Scripting entries via the Web user Interface were restricted in release 5.1
CVE-2016-0734 "Clickjacking"	Resolved in the 6.2 release.
"Beast" and "Logjam"	The "Beast" and "Logjam" vulnerabilities have been addressed in the 6.3 release.
TLS 1.0 access	TLS 1.0 has been disabled so only newer versions are used. This was addressed in the 6.3 release.
"Sweet 32 Birthday Attack"	Vulnerability Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) resolved in the 7.0 release.
TLS 1.1 access	TLS 1.1 has been disabled. TLS 1.2 is the minimum version used. This was addressed in the 7.6 release.
CVE-2004-0583 Lack of Account Lockout	This vulnerability could allow a brute force ID/Password attack. This was addressed in the 7.8 release. The account lockout time is 15 minutes. If login is attempted during the timeout period, the timeout period will restart.
California IoT Security Law; SB-327	User must now configure unique administrator credential to access the card. This was addressed in the 7.8 release.

4. Update Instructions

The Unity cards may be updated to this firmware version using the web-based Firmware Upload feature. Please refer to the Firmware Updates and Card Configuration sections of the [Liebert IntelliSlot Unity Card User Manual \(SL-52645\)](#) and the [Mass Firmware and Configuration Update Tool](#)

It is recommended to change the following six (A-F) security related configuration settings to non-default values before updating to 7.8.0.0 and later firmware version. When updating many devices, the mass configuration tool can be used for convenience. If these configuration settings already contain non-default values, then please proceed with the firmware update.

- A. Administrator username to a non-default name
- B. Administrator password to a non-default password
- C. General User username to a non-default name
- D. General User password to a non-default password

Local Users: Table

Updated: Jan

[Click here to edit columns displayed in the table](#)

Report	User Name	User Password	Authorization for User
Local Users [1]	trebeiL	*****	Administrator
Local Users [2]	resu	*****	General User
Local Users [3]			No Access
Local Users [4]			No Access
Local Users [5]			No Access
Local Users [6]			No Access
Local Users [7]			No Access
Local Users [8]			No Access
Local Users [9]			No Access
Local Users [10]			No Access

- E. SNMP Community String to a non-default community string

SNMPv1/v2c Access: Table

Updated: January 14, 2020 02:51:04PM

[Click here to edit columns displayed in the table](#)

Report	SNMP Access Host	SNMP Access Type	SNMP Access Community String
SNMPv1/v2c Access [1]	10.20.30.40	Read/Write	*****
SNMPv1/v2c Access [2]		Read Only	

- F. Enable Password Protected Site

Web Server:		Updated: January 14, 2020 02:55	
Settings		Edit	Save Cancel
Web Server Protocol	HTTP		
HTTP Port	80		
HTTPS Port	443		
Password Protected Site	<input checked="" type="checkbox"/> enabled		
Remote Write Access	<input checked="" type="checkbox"/> enabled		
Session Idle Timeout	5		

If the security related configuration items (A-F) identified above contain default values when updating to 7.8.0.0 and later firmware versions – then manual completion of the following two dialogues will be required.

- 1) The “Please Create an Administrator Level Account” dialogue is presented when the following configuration setting are true on an existing card that will be firmware updated:
 - a. Username = Liebert
 - b. Password = Liebert
 - c. Authorization for User = Administrator

This is a one-time requirement that must be completed in order to access the card.

The following progress messages will appear in the dialogue after clicking the “Add User” button:


- “Waiting on response from server”
- “Administrator user added. Waiting 3.5 minutes for reboot” (Only when updating a card)

Please note that if this is a new card with v7.8.0.0 and newer firmware, the following dialogue is mandatory.



Please Create an Administrator Level Account

Username

Password
 

Confirm Password

The card security has been updated to align with current best practices.

-
- 2) The **“Recommended Security Updates”** dialogue will be presented when one or more of the following configuration settings are true:
- Username is “User” and Password is “User” and Authorization for User is “General User”
 - SNMP Community String is “LiebertEM”
 - Site Protection is disabled

It is strongly recommended that non-default configuration settings be used for maximum security.

If you wish to retain your existing configuration settings, they must be reentered and saved in this dialogue. If a setting is left blank, then it will be deleted.

The following progress messages will appear in the dialogue after clicking the “Save” button:

- “Waiting on response from server”
- “Administrator user added. Waiting 3.5 minutes for reboot” (Only when updating a card)



Recommended Security Updates

The card security has been updated to align with current best practices.

Please add a User Level Account (optional)

An existing default User Level account will be deleted.

Username

Password

Confirm Password

Please add an SNMP Access Community String (optional)

Any existing default SNMP Community string will be deleted.

Community String

Password Protect Site

Password Protected Site mode is **strongly recommended**. This mode requires a user login to access the web pages.

Site Protection ☒

Saves all changes and restarts the card

Save

5. Known Issues

Component	Description
Device Settings	When temperature settings are made on some thermal devices, there may be some 'round-off' error of one tenth of a degree between what was requested and what the device shows after the change. This is a known limitation of some thermal device firmware versions and will be corrected in future versions of the device controller firmware.
Liebert GXT3/4 UPS Support	The IP address of the Unity card may be displayed on the local display of the Liebert GXT4 UPS unit. The IP address is pushed to the GXT4 when the card starts up. If the address changes (for example, if it is changed by the DHCP server when the DHCP lease runs out), the local GXT4 display will continue to show the old address until the card is restarted.
	While the SNMP OIDS for the GXT are backward compatible with those from the IS-WEBCARD, the text values in some SNMP varbinds and email/SMS notifications have changed slightly to use the Unity card equivalent.
Sensor Support	The preferred way to change the display order for multiple sensors is through the Web user interface. If the order is changed using one of the supported protocols then the entire list of sensors should be set in the correct order (including slots that should become blank) to ensure all sensors are still included.
SNMP	SNMP <i>getnext</i> requests may fail on some tables if there are multiple varbinds in the request. If this occurs, use single-varbind requests.
Firmware Update	When using the Microsoft Edge browser to upgrade firmware from a 7.5.0.0 or 7.5.1.0 to another release, the web page will become blank and display an authorization error. To recover, enter the IP address of the card followed by <Enter> after the firmware upgrade completes (this typically takes 5 – 6 minutes).
Firmware Update	An update from version 4.3 or older will fail when updating to the v7.7 release or newer. An intermediated (two step) process is required - update to V7.6, then update to v7.7 or newer. Please contact Monitoring Application support to obtain the 7.6 firmware version.