Liebert® IntelliSlot™ Unity Card
Version 8.0.0.1_00101 Firmware
December 11th, 2020

This document outlines:
1. Version and Compatibility Information
2. What's New
3. Security Issues Addressed
4. Upgrade Instructions
5. Known Issues
6. Previous Release Updates and Enhancements

==========

1. Version and Compatibility

==========

This release contains the following firmware version:

IS-UNITY_8.0.0.1_00101

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 APM
Liebert APM160
Liebert APS
Liebert CRV
Liebert CRV/iCOM Edge
Liebert CW*
Liebert CWA
Liebert Challenger*
Liebert DataMate
Liebert Deluxe System/3*
Liebert DCL
Liebert DCP
Liebert DP400
Liebert DS*
Liebert DSE
Liebert EPM
Liebert EXC
Liebert eXL
Liebert EXL S1
Liebert eXM
Liebert EXM2
Liebert FDC
Liebert FPC
Liebert GXE2
Liebert GXT3 / GXT4
Liebert HPC-S,M,R,W,Generic
Liebert HPM
Liebert ITA2/EXS
Liebert Mini-Mate
Liebert NX 225-600kVA
Liebert NXC
Liebert NXL
Liebert NXR
Liebert PCW
Liebert PDX
Liebert PeX*
Liebert PPC
Liebert PSI5
Vertiv™ Edge
Liebert RDC
Liebert RX
Liebert STS2
Vertiv™ Trinergy Cube
Liebert XDC with iCOM™ Control
Liebert XDP with iCOM™ Control
Liebert XDP-Cray
Liebert XDU
Liebert XDM

*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 Edge – ver 44.17763.831.0 / 17763.1457 or later
- Microsoft IE 11 – ver 11.0.175 / 17134.1304 or later
- Mozilla Firefox® - ver. 71.0.1 or later
- Google Chrome™ – ver. 85.0.4183.102 / 18363.1082 or later
- Safari® (MacBook®) - ver. 13.1.2 / Catalina 10.15.6
- Safari® (iPad®) - ver. 7.1

==========

2. What's New

==========

This release contains the following enhancements, updates and corrections:

- Corrected the "Generate Self-Signed SSL Certificate" functionality

==========

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.
CWE-521 Password Complexity	Minimum of 8 to a maximum of 30 case-sensitive, printable characters (excluding: \’<>~?#, double quote and space. Also, must contain a combination of upper and lower case, digit and special characters. The password cannot contain the User Name.
CVE-2018-0459 Authorization Management	This vulnerability could allow an unauthorized (non-admin) user to make changes to the card configuration

==========

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

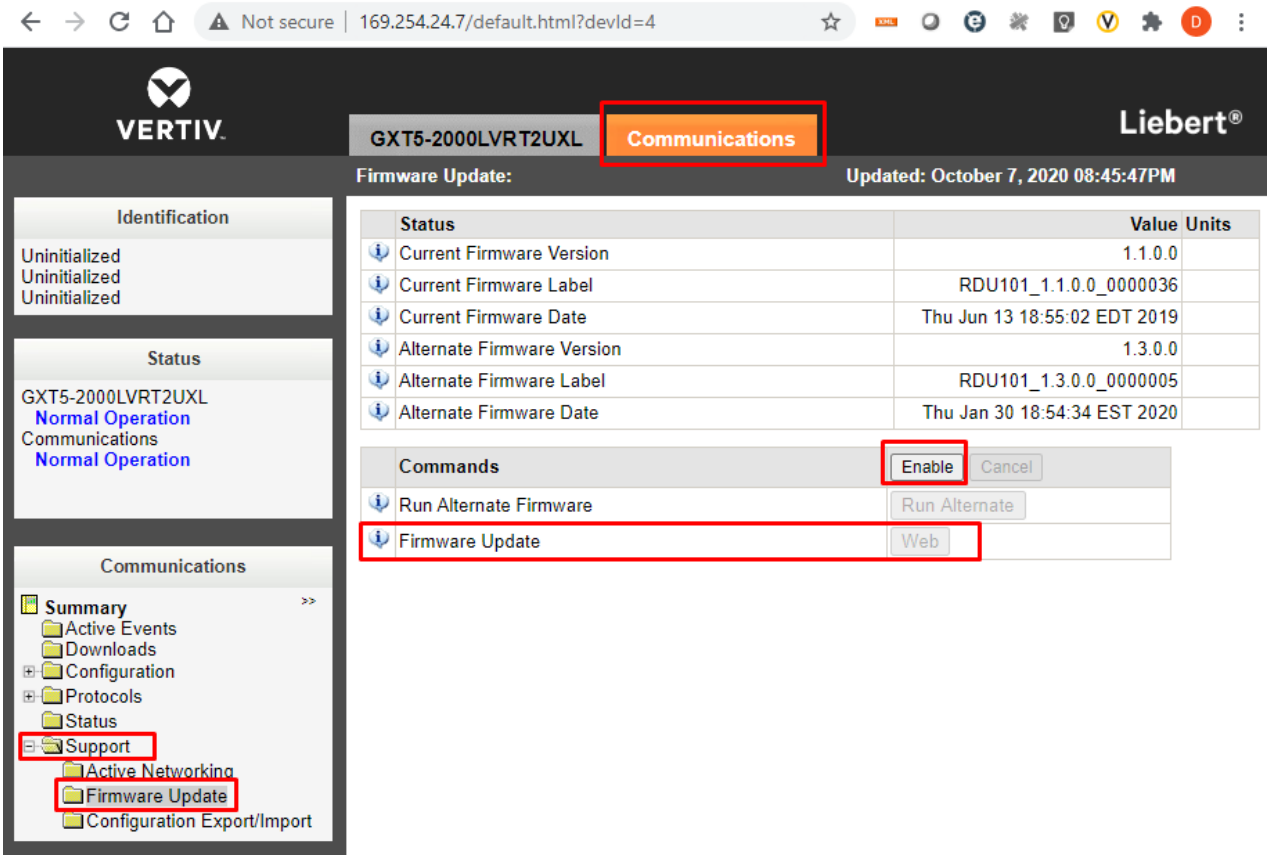
1) **Connecting to the card**
After installing the card, allow time for the card to boot. Connect an Ethernet cable from the card to a PC or Laptop. A link local connect can be established. This is a direct PC-to-card Ethernet connection. The PC acquires a local address and the card is accessed at 169.254.24.7. Please consult the Quick Start Guide and User Guide for further details if needed.

2) Open a web browser (such as Chrome) and enter 169.254.24.7 in the address bar.

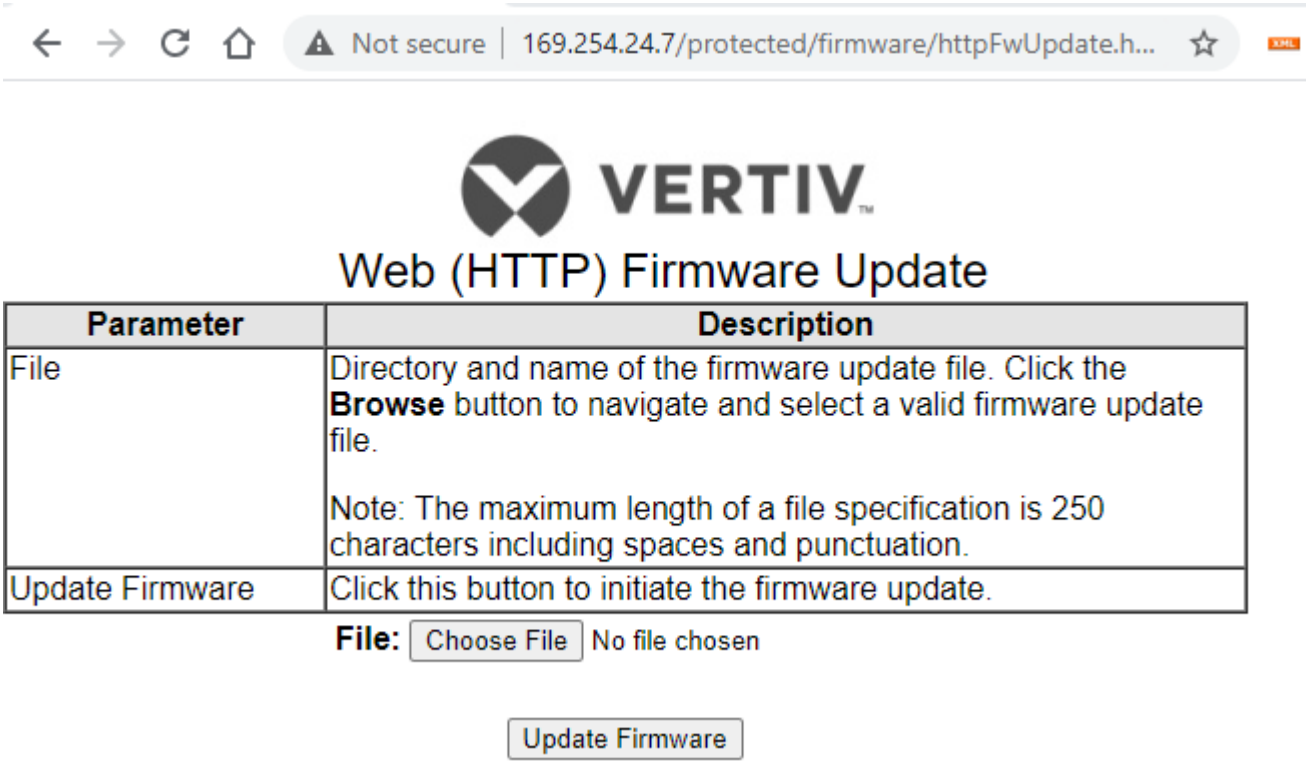
3) Update the card firmware.

Navigate to:

a. "Communications" tab
b. "Support" folder
c. "Firmware Update" folder
d. Click "Enable"
e. Click "Web"

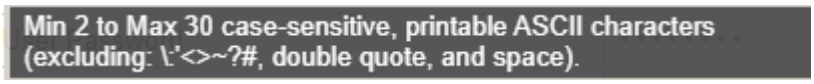


4) The Firmware Update page will appear.
   a. Use the “Choose File” button to select the firmware file via Windows File Explorer.
   b. Click the “Update Firmware” button.



5) Following the firmware update, the **“Please Create an Administrator Level Account”** dialogue will appear in the browser.
   a. The customer will provide the credentials.
      -or-
   b. The installer can choose/create the credentials. The credentials must be communicated to the end customer.

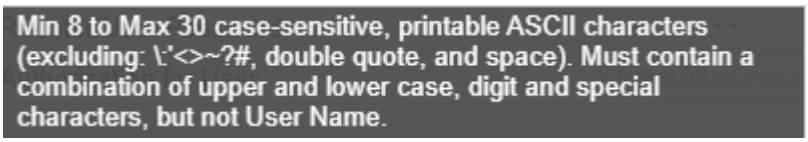
User Name – Allowable characters



Minimum of 2 to a maximum of 30 case-sensitive, printable characters

(excluding: \’<>~?#, double quote and space.

Password – Allowable characters

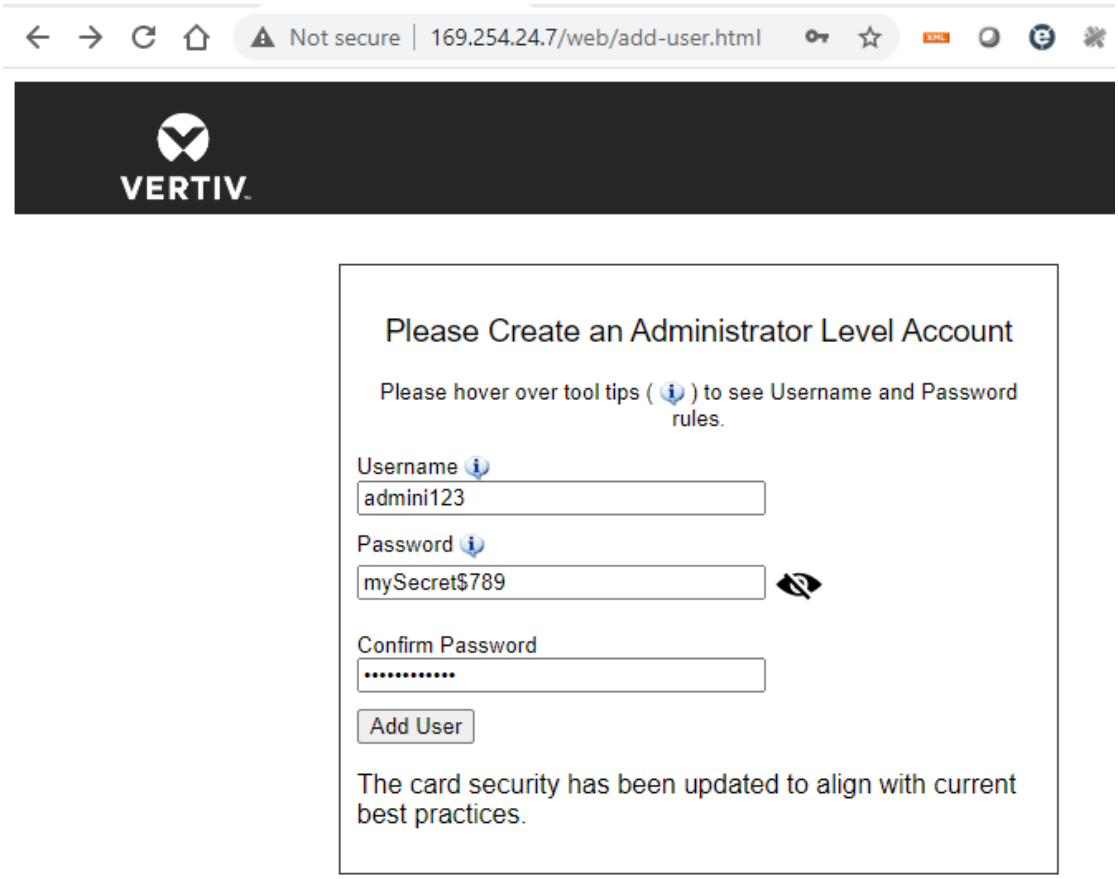


Minimum of 8 to a maximum of 30 case-sensitive, printable characters (excluding: \'<>~?#, double quote and space. Also, must contain a combination of upper and lower case, digit and special characters. The password cannot contain the User Name.

6) Create an Administrator account as shown in the ***example*** below:

Username = admini123

Password = mySecret$789



7) Take careful note of the ***actual credentials*** that are entered in the dialogue shown above.

Note: If the Administrator credentials are lost or forgotten, the card must be reset to a Factory Default state to regain access. Please reference the User Guide for instructions to reset the card.

8) Click **"Add User"**.

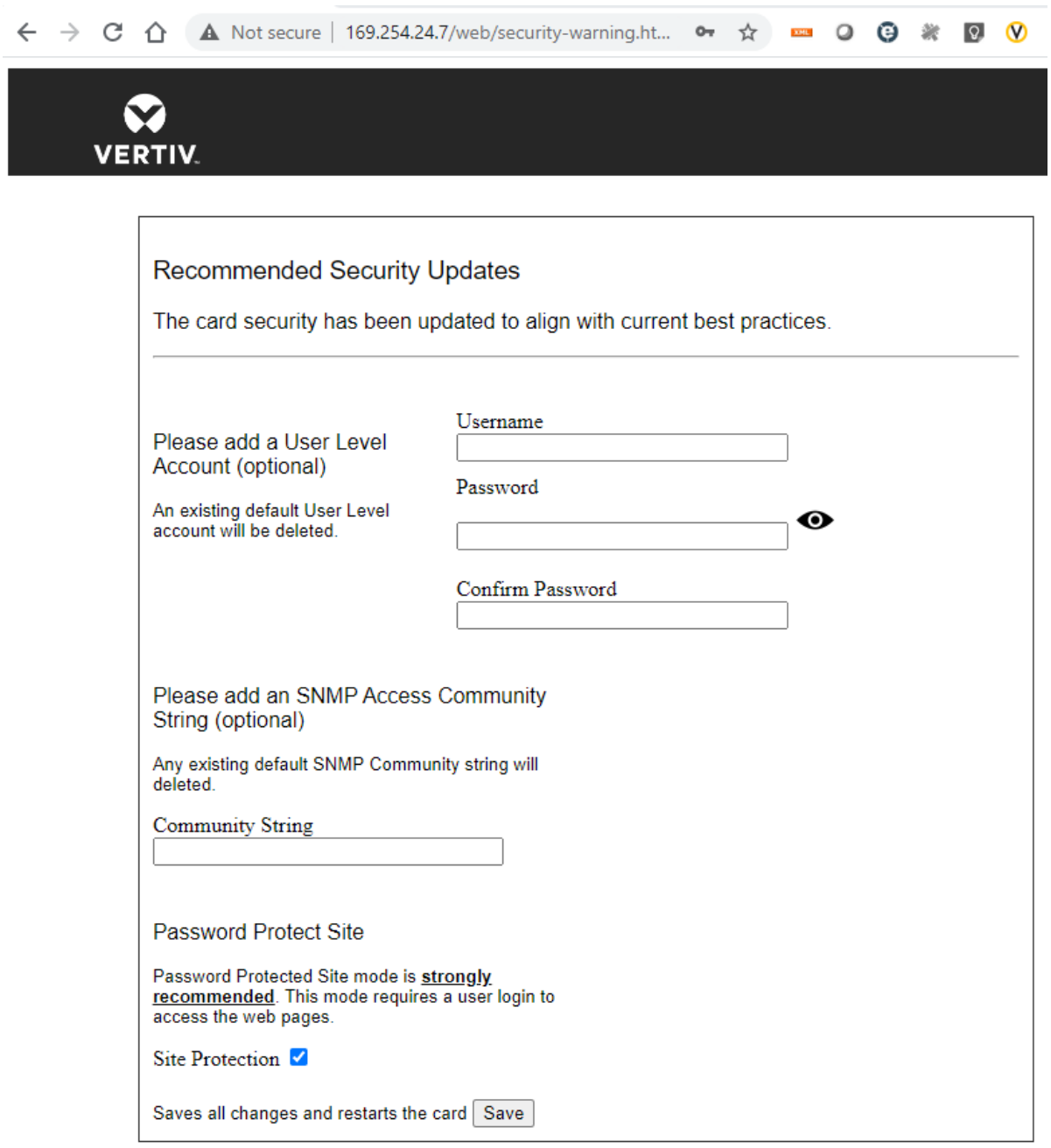
9) The dialogue will briefly indicate - "Waiting on response from server……."

10) Next, the dialogue will briefly indicate – "Applying Updates…."

Note: Do not click the "Back" button in the web browser

If the card appears to be unresponsive in the web browser at any point, please re-enter the 169.154.24.7 in the address bar.

11) A second dialogue – **"Recommended Security Updates"** may appear. If it does, just click the **"Save"** button at the bottom to continue.

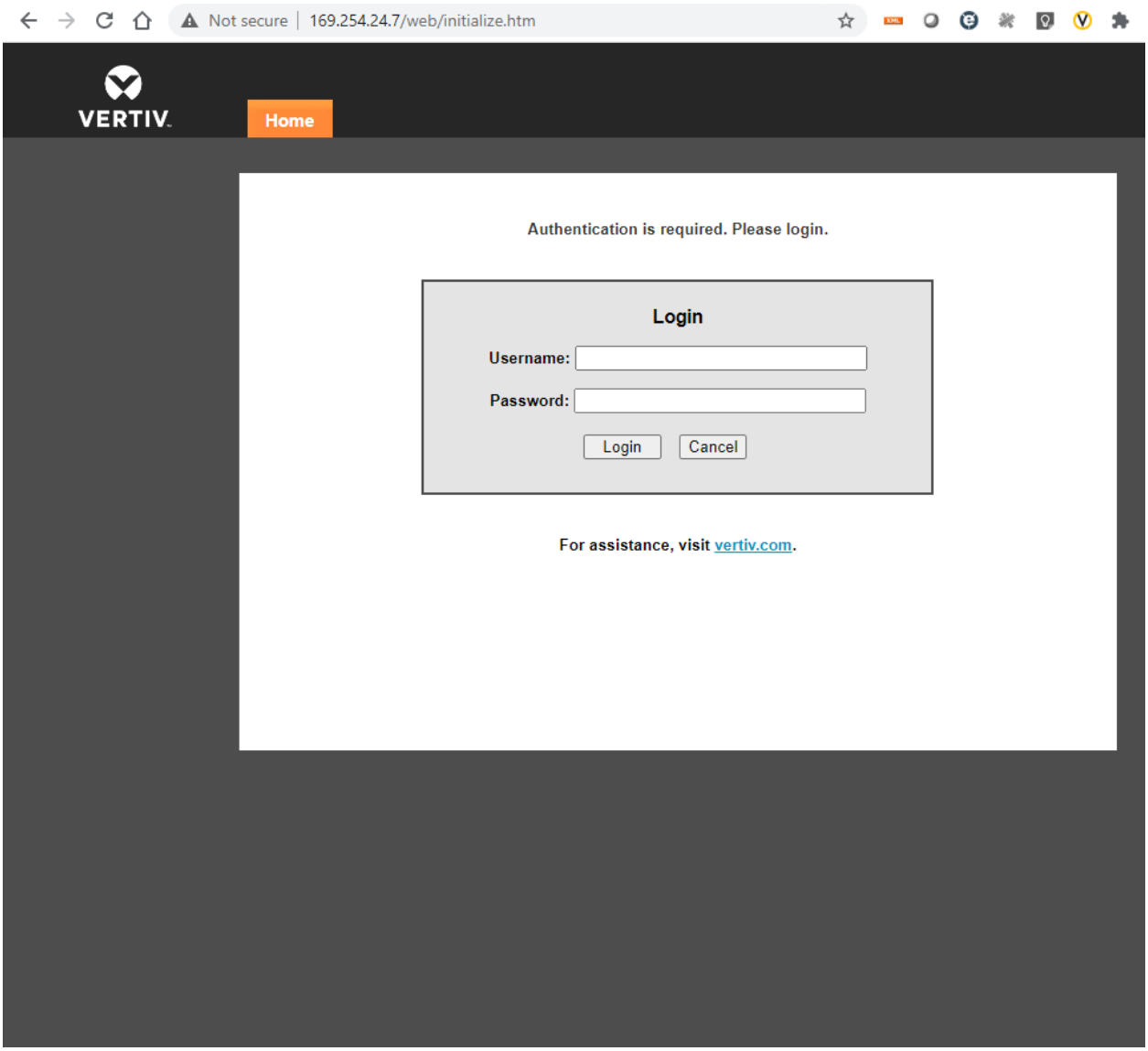


12) The dialogue will briefly indicate - “Waiting on response from server…….”

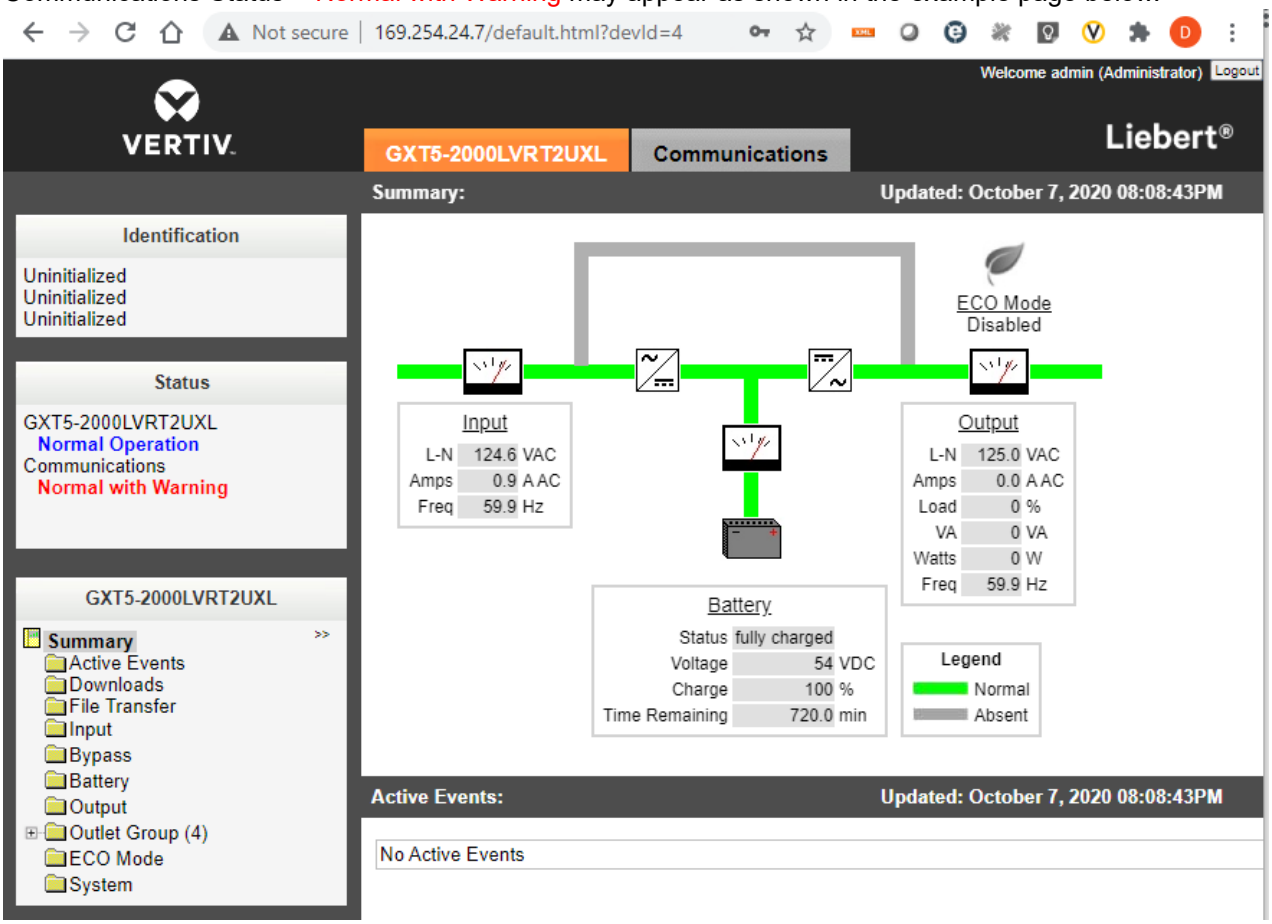
13) The Password Protected Site login screen is presented. Please login with the administrator credentials created p above. Please reference step 7)

Username = xxxxxxxxxx

Password = xxxxxxxxxxx



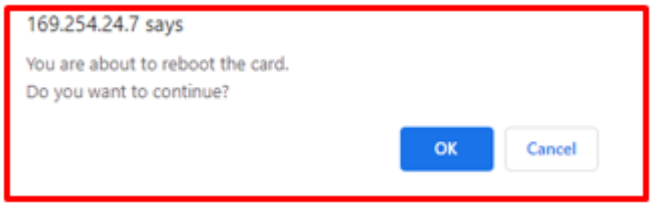
14) Communications Status = Normal with Warning may appear as shown in the example page below.

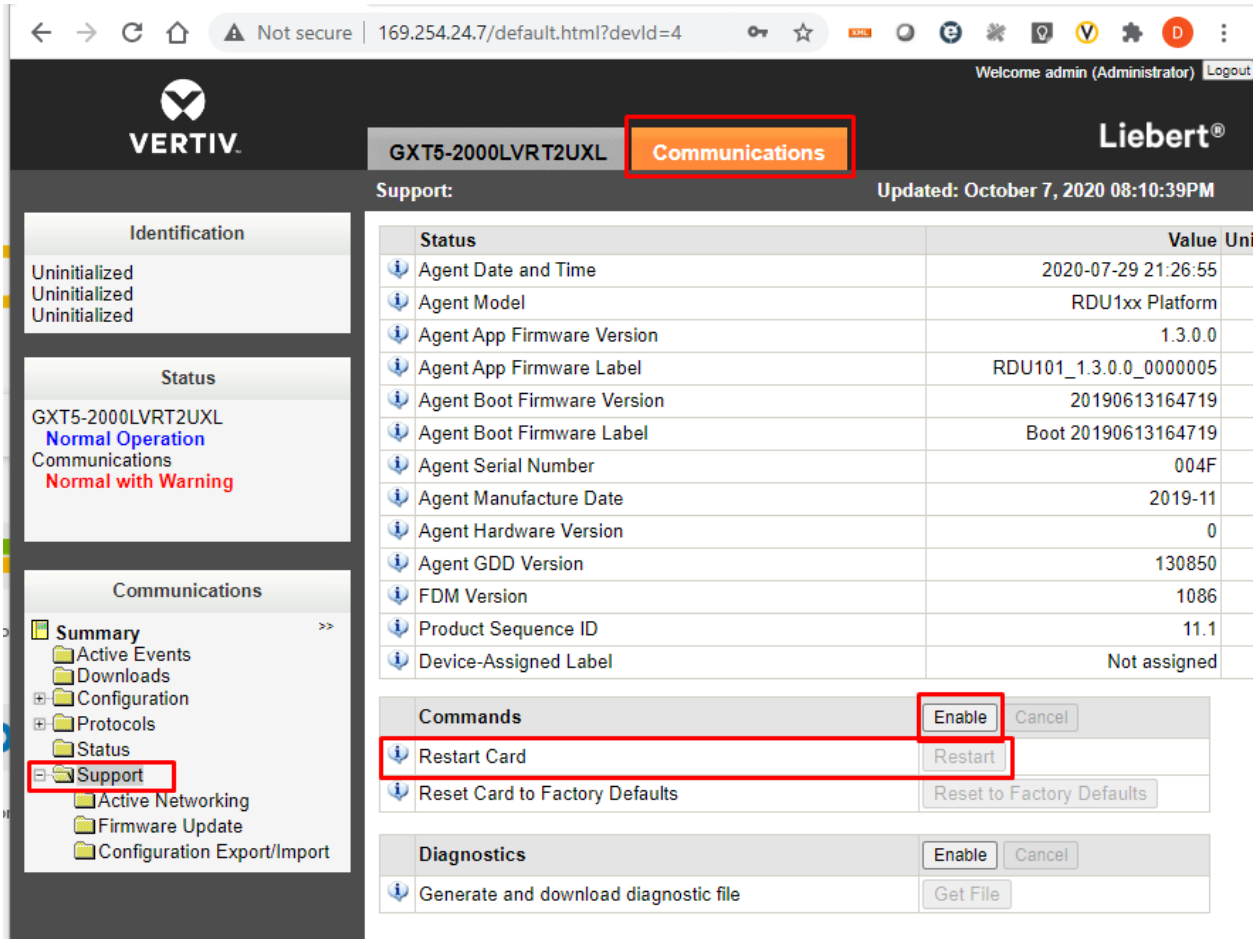


15) The Normal with Warning message can be cleared by **Restarting** the card.

Navigate to:

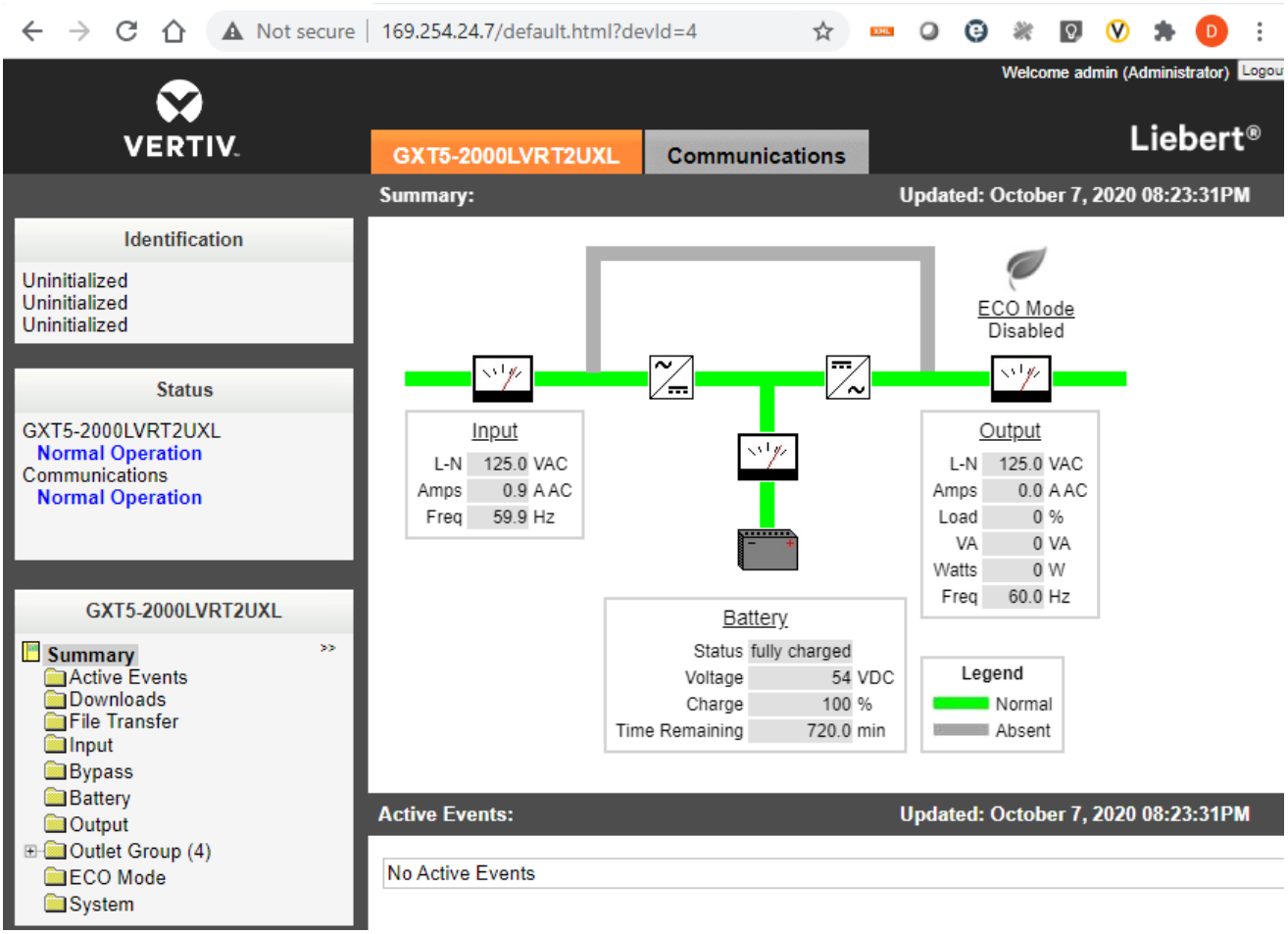
a. “Communications” tab
b. “Support” folder
c. Click “Enable”
d. Click “restart”
e. Click “OK” in the browser pop-up dialogue





16) Following the card restart, login to the card again (same as step 10) above.

17) The card web page will be normal as shown below



18) **The administrator account setup is complete.**

==========

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 ***getnext*** 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.
Account Lockout	If Remote Authentication is enabled with Local Authentication, Example: **RADIUS then Local.** The Local User will be locked out after three successful logins. The local user must wait 15 minutes to login again.
Firmware Update	Firmware update is not functional with Firefox running on Windows. However, it is successful running on Ubuntu Linux

==========

6. Previous Release Updates and Enhancements

==========

Component	Description

v7.0.1.0	This release contains the following enhancements:
	• Configuration Import / Export
	  ○ Manual import / export is supported via the web UI.
	  ○ Mass (programmatic) import / export is supported via an HTTP (specification is available).
	• Remote Authentication
	  ○ LDAP
	  ○ RADIUS
	  ○ TACACS+
	  ○ Kerberos
	• Support for new Devices
	  ○ iCOM DP400
	  ○ Liebert ITA2
	• EXL S1 legacy modbus mapping support Input/Bypass/Output voltages.
	
	The following issues were addressed in this release:
	• If the administer User Name = “admin” was used prior to upgrading to Version 7.0.0.0, the user would be no longer have write access to the card. Reset to factory default was required to restore write access to the card.
	• If a user upgraded to version 7.0.0.0 and never changed the default administrator credentials in cards that were originally shipped with version 5.0.0.0 or earlier, the Users entries would become corrupted. Reset to factory default was required to restore write access to the card.

v7.1.0.0	This release contains the following enhancements:
	• (40xxx) support Input/Bypass/Output voltages.
	• BACNet COV persistence.
	• The following issues were addressed in this Configuration Import / Export
	  ○ Manual import / export is supported via the web UI. and programmatically using HTTP (specification is available).
	  ○ Mass (programmatic) import / export is supported the web UI and programmatically using HTTP (specification is available).
	• Remote Authentication

Component	Description
	○ LDAP ○ RADIUS ○ TACACS+ ○ Kerberos • Support for new Devices ○ Liebert DP400 ○ Liebert ITA2 ○ Liebert STS2 EXL S1 legacy modbus mapping release: • If the administer User Name = “admin” was used prior to upgrading to Version 7.0.0.0, the user would be no longer have write access to the card. Reset to factory default was required to restore write access to the card. • If a user upgraded to version 7.0.0.0 and never changed the default administrator credentials in cards that were originally shipped with version 5.0.0.0 or earlier, the Users entries would become corrupted. Reset to factory default was required to restore write access to the card. • The card could fail to write admin credentials to the file system following a restart. Hard restart of the card (remove and restore power) was required to regain access.
v7.2.0.0	This release contains the following enhancements: • Support for new NOR Flash (previous part is obsolete) • Support for new NAND Flash (previous part is obsolete) • IPv4 Network address configuration via the diagnostics console (implemented for Apple Retail)
v7.3.0.0	This release contains the following enhancements: • PSI5 UPS support • GXE2 UPS support • 2 - Factor RSA support for Remote Authentication • Configurable DNS Hostname
v7.3.1.0	This release contains the following enhancements: • Add the following data points for EXL S1 ○ Bypass Input Current Phase A ○ Bypass Input Current Phase B ○ Bypass Input Current Phase C

Component	Description
v7.5.0.0	This release contains the following enhancements: • Add the support for Mini-Mate 2, DataMate and EXS Frame 2 and Frame 3
v7.5.1.0	This release contains the following enhancements and corrections: • Change firmware to eliminate Modbus 65535 response data during device discovery. • Correct an alarm latching behavior when monitoring the STS2 Static Transfer Switch.
v7.6.0.0	This release contains the following enhancements and corrections: • EXL S1 – Increase battery cabinet support to 8. • NXL – New fan and thermal data points. • APM600 and eXM MSR – Add Lithium Ion Battery support. • PSI5 – Add outlet reboot capability • Disable TLSv1.2 support
v7.6.1.0	This release contains the following enhancements and corrections: • EXL S1 – YDN23
v7.7.0.0	This release contains the following enhancements, updates and corrections: • CRV/PACC • APM NXr • EXL S1 • iCOM PA XDU • ITA2_8K
v7.8.0.0_83	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 • Account lockout for 15 minutes after 3 failed login attempts
V7.9.2.0	This release contains the following enhancements, updates and corrections: • Corrected an unintended reboot condition when a BACnet/MSTP BMS was in use.

Component	Description
	• Trinergy Cube *initial release* • iCOM EDGE CR012 • iCOM EDGE CR025 • iCOM EDGE CR030 • iCOM EDGE PeX4 • iCOM CWA • iCOM XDU • EXL-S1
V8.0.0.0	This release contains the following enhancements, updates and corrections: • EXM2 • APM160 • XDM • LLDP protocol support • Password Complexity implemented • Authorization Management Vulnerability mitigated