Network Management Card 4 (NMC 4) Galaxy VL Firmware 13.18.1 Release Notes

Table of Contents

New Features....1
Fixed Issues....1
Known Issues....2
Miscellaneous....4
PowerNet MIB Reference Guide....4

The Galaxy VL application firmware version 13.18.1 release notes apply to the following cards and products:

- GVL200K500DS, GVL300K500DS, GVL400K500DS, GVL500KDS
- AP9644 Network Management Card 4 (NMC4)

New Features

For a list of features available in the NMC 4, refer to the Network Management Card 4 Feature List.

Top ↑

New Feature
Additional logging has been added for the following features: TCP/IP, EventActions, SSH, Web, FTP, System, SNMP and Modbus.
All user types can now change their own password via the Web UI and CLI. **Note:** Admin users can no longer change their own password without first entering their current password on the Web UI and CLI. It will however be possible for an Admin user to change another users password **without** entering the current password.
UPS ambient temperature is now readable from an NMC over Modbus.

Fixed Issues

Top ↑

Fixed Issue
From the Galaxy VL Firmware v12.21 release, there were cybersecurity fixes resolving vulnerabilities with vertical privilege escalation, File Enumeration, and HTTP Denial of Service. The most recent release, Firmware v13.18.1 also contains a security fix for a CVS injection and a directory transversal vulnerability issue.
It is now possible to generate a Technical Support debug file if you are logged into the NMC via RADIUS. You no longer need to log in as a local user to generate this file.

Known Issues

Top ↑

Known Issue
Traps with more than 200 characters are being truncated.
New additional logs are not translated for the syslog messages.
Configuration changes for Vendor Cookie sections are not reported in emails.
Due to security enhancements, downgrading to a previous firmware version may result in some features not working as expected. If a downgrade to a previous firmware version is required, the email authentication password will need to be reset manually.
Some DER format certificates cannot be uploaded to the NMC using SCP. It is recommended that PEM format certificates are used.
As user SSL certificates are removed, and self-signed certificates are regenerated during a reset of all NMC settings, when you are logged out after initializing a reset of all NMC settings, you must refresh the page before the browser can connect to the NMC over HTTPS using the new SSL certificates.
After a reset of all NMC settings, you may be presented with the error “Maximum number of sessions exceeded” when attempting to login to the NMC Web UI. The NMC should be accessible once again after 3 minutes.
Events related to the temperature and humidity probe connected to the Network Management Card are not displayed in PowerChute Network Shutdown if the probe is connected after registration is complete. To prevent this issue from occurring, connect the temperature and humidity probe to the Network Management Card before completing the registration in PowerChute Network Shutdown. Alternatively, connect the probe after registration is complete and restart the PCNS service.
When you attempt to login to the NMC Web UI following a soft reset, you will be immediately logged out following a successful login. This can be resolved by closing and restarting the web browser.
When using a custom email server for a configured email recipient, if a recipient authentication password is set for the email recipient, the settings for the recipient can no longer be changed using the `email` CLI command, unless the password `(-p)` and confirm password `(-d)` arguments are included. Note that the settings can be changed without any problems from the Web UI.
On very rare occasions following a soft reset, when SNMP is configured, the NMC does not communicate over SNMP. On these occasions, a reboot of the NMC is required to resolve the issue. With some browsers, due to auto-refresh functionalities, an inactive user may not be automatically logged out if the configured session timeout is greater than 15 minutes. It is recommended that the session timeout for a user is no greater than 15 minutes. The default is set to 3 minutes.
SSH and HTTPS connections will be unsuccessful if the private key is not generated in PEM.

Known Issue
It is not possible to register a PowerChute client that is using IPv6 with the NMC.
Disabling Syslog on a per-event basis does not work as expected. You can only disable Syslog using the event action per-group option in the Web UI.
No event is logged when an SSL certificate is removed via the **SSL Certificate Configuration** page in the Web UI. The “New self-signed certificate loaded” event will be logged if a new certificate is manually added or auto generated if the old certificate is deleted or out of date.
You may be logged out unexpectedly from the Web UI if multiple Web UI tabs are open. This issue only occurs on Google Chrome.
When a user’s password is changed via the `user` command in the CLI and does not meet the password requirements, a parameter error is displayed instead of “Password did not meet the requirements for a strong password.”
There are discrepancies between the current time displayed in the Web UI and the CLI. The `date` command in theCLI will report the current time in real-time, whereas the Web UI will display the browser’s current time with respect to the UTC value set. **NOTE:** The UPS HMI will also display the current time in real-time.
The **Configure Events** screen in PowerChute Network Shutdown v4.3 displays the “Communication Established with EMC” and “Communication Lost with EMC” events. These events can be ignored as they are not supported.
When the optional NMC (AP9644) is inserted, some alarms and events are not logged on all the configured interfaces (traps, emails, Syslog, Event Log). For example, the “Lost Communication” alarm is not logged as an active alarm or sent as a trap/email.
When the Web UI is locally accessed via an internal IP address (169.254.251.1 / 169.254.252.1) and HTTP/HTTPS is disabled, you can no longer access the UI using the disabled protocol. For example, if HTTP is disabled, you cannot access the Web UI at http://169.254.252.1
When adding a rule via the **Firewall Configuration** page in the Web UI, the table incorrectly includes the Range/Subnet column, which is not currently supported.
The Notification Delay and Repeat Interval features for event actions do not behave as expected. For example, you may receive multiple notifications for an active event.
You cannot connect to SNMPv1 using an IPv6 address. Use SNMPv3 as an alternative.
When you log out from the NMC serial console interface, the Current Sessions page in the Web UI still shows the session as active.
File Transfer Protocol (FTP) is not available over IPv6.
When credentials are provided in StruxureWare Data Center Expert after adding the NMC via SNMP, the NMC still requires login credentials when attempting to access the Web UI.

Known Issue
When Auto Configuration is disabled in the IPv6 Settings page in the Web UI, the NMC still displays the card's IPv6 address, and the card is accessible using a DHCP IPv6 address.
No browser warning message is displayed in the Web UI when navigating without saving your changes.
When viewing the Event Details page in the Web UI for an event, you cannot disable the logging of an event to the Event Log.
When accessing the Web UI using a smartphone, the Rule Configuration table on the Firewall Configuration page is not responsive.
When an SNMPv3 profile is enabled with a valid NMS IP/Host Name, you can connect to a MIB browser of another system and not the configured SNMP profile. **NOTE:** The only supported value for **NMS IP/Host Name** for SNMPv3 is "0.0.0.0".

Miscellaneous

Recovering from a Lost Password

If you forget the Super User password, you can reset it back to its default of `apc` by holding down the Reset button on the NMC's faceplate for 15 seconds. The NMC's Status LED will flash orange three times in a short burst to indicate that the reset was successful. This action is logged to the Event Log.

Alternatively, you can reset the Super User password back to its basics in the Web UI (**Control > Network> Reset NMC Settings**) or through the CLI interface (`resetToDef`). To reset the Super User password, Administrator, or Network user privileges are required. Reset-related actions are logged to the Event Log.

Event Support List

To obtain the event names and event codes for all events supported by a currently connected device, first retrieve the config.ini file from the attached NMC. To use SCP to retrieve config.ini from a configured NMC:

1. Open a connection to the NMC, using its IP Address:

   scp <admin_username>@<ip_address>:config.ini <filename_to_be_stored>

2. Log on using the Administrator user name and password

   The file is written to the folder from which you launched SCP.

   In the config.ini file, find the section heading [EventActionConfig]. In the list of events under that section heading, substitute 0x for the initial E in the code for any event to obtain the hexadecimal event code shown in the user interface and in the documentation. For example, the hexadecimal code for the code E0033 in the config.ini file (for the event "System: Configuration change") is 0x0033.

PowerNet MIB Reference Guide

NOTE: The MIB Reference Guide on the Schneider Electric website explains the structure of the MIB, types of OIDs, and the procedure for defining SNMP trap receivers. For information on specific OIDs, use a MIB browser to view their definitions and available values directly from the MIB itself. You can view the definitions of traps at the end of the MIB itself (the file powernet440.mib or higher on the Schneider Electric website).

http://www.se.com

990-6147P-001

03-2024