

Network Management Card 4 (NMC 4) Galaxy VS Firmware 6.123.0 Release Notes

Table of Contents

New Features.....	1
Fixed Issues	1
Known Issues	2
Miscellaneous.....	5

The Galaxy VS application firmware version 6.123.0 release notes apply to the following NMC cards and products:

- **AP9644 Network Management Card 4 (NMC4)**
- See Knowledge Base article [FAQ000265832](#) for the list of applicable SKUs.

New Features

For a list of features available in the NMC 4, refer to the [Network Management Card 4 Feature List](#).

[Top ↑](#)

New Feature
No new features in this release.

Fixed Issues

[Top ↑](#)

Fixed Issue
An issue has been fixed that addressed a potential NMC reboot when using SNMP for an extended period.
The loading icon no longer continuously displays on the EAPoL Configuration page when an existing CA certificate is removed.
Self-signed certificate generation on the Web UI will no longer fail if the page is refreshed, or you navigate to a different page while the regeneration process is in progress.
Previously users may have experienced an issue following an NMC soft reset via the Web UI where a certificate failed to be generated, preventing access to the Web UI. This issue has now been addressed.

Fixed Issue
Security Update
The following third-party component (open source or proprietary) has been updated to address a cybersecurity vulnerability: - Unauthenticated Remote Code Execution in Erlang/OTP SSH - CVE-2025-32433 Erlang OTP library has been updated to a patched version to mitigate this issue.

Known Issues

[Top ↑](#)

Known Issue
Commands are displaying twice on the CLI.
Following a reset of all configuration changes, except for the TCP/IP settings, NMC Modbus TCP remains in the enabled state and allows new connections. To resolve this issue, disable Modbus from the Web UI and apply the settings. The Modbus TCP feature will then be disabled and will not allow new connections.
Email notifications routed through Gmail are not being received by end users. Where feasible, consider using an alternative email service for critical communications.
Changes made to the date and time on the Network Management Card through the Web Interface are not always applied the first time. If this happens, try to hit the apply button again, refresh the page, or navigate away to another page for the change to be applied.
An error message is not displayed when an invalid certificate is uploaded through the Web Interface. A warning icon appears but there is no error message or event logged.
Warning sign is displayed when the user uploads a valid EAPOL certificate. The certificate is however uploaded successfully.
Email notifications are not working when the SMTP server is configured to use an IPv6 address.
Syslog notifications are not working when the Syslog server is configured to use an IPv6 address.
SNMP Traps are not working with Global, Static and Link-Local IPv6 addresses.

Known Issue

When a reset is performed or self-signed TLS certificates are generated from the Web UI or the CLI on the Network Management Card on the 29th of February, HTTPS may become unavailable as an invalid TLS certificate will be created. We recommend you wait until the 1st of March on a leap year to run the `gencert` command on the Network Management Card CLI. If browsing over the Web UI is essential, the Network Management Card can be accessed over HTTP, however for cybersecurity reasons, we at Schneider Electric do not recommend this unless absolutely necessary.

Traps with more than 200 characters are being truncated.

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.

Configurable 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 the CLI 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.

File Transfer Protocol (FTP) is not available over IPv6.

When credentials are provided in EcoStruxure IT Data Center Expert after adding the NMC via SNMP, the NMC still requires login credentials when attempting to access the Web UI.

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.

Known Issue
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

Top ↑

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 powernet457.mib or higher on the [Schneider Electric](#) website).

Copyright © 2025 Schneider Electric. All rights reserved.

<http://www.se.com>

TME39546D

07-2025