

Datacom Systems Inc.

9 Adler Dr.

East Syracuse, NY 13057

Phone: 315-463-9541

Support: support@datacomsystems.com

Firmware for:

SS-2222-CM3-10G

SS-2222-CM2-10G

SS-2222-LR-10G739

SS-2222-CM1-10G

SS-2222-CM-10G

SS-2222-SR-10G735

SS-2212-CM3-10G

SS-2212-CM2-10G

SS-2212-LR-10G739

SS-2212-CM1-10G

SS-2212-CM-10G

SS-2212-SR-10G735

Browsers supported for GUI: Mozilla Firefox 15, Microsoft Internet Explorer 9.0

Dromis.7 (SVN 2474)

New Features Added

1. Added a browser based graphical user interface.
2. Added SNMP Support.
3. Added RADIUS Support.
4. Added TACACS+ Support.
5. CLI – Command Line Interface.
 - a. Added relevant commands for New Feature (SNMP, RADIUS, TACACS+ and Authentication Order).
 - b. General improvements of commands.

Notes and Limitations:

1 Stacking

- 1.1. For stacking to function properly all devices must have the same firmware version.

2 CLI and GUI

- 2.1. (FB1580) The following characters should not be used for names or descriptions:

- 2.1.1. Curly brackets (braces) { }
- 2.1.2. Backslash \
- 2.1.3. Pipe |
- 2.1.4. Tilde ~
- 2.1.5. Number sign #
- 2.1.6. Grave accent `
- 2.1.7. Quotes “
- 2.1.8. Apostrophe ‘
- 2.1.9. Colon :

These characters may cause inconsistent displays, or misinterpreted entries.

- 2.2. GUI supports only encrypted web sessions (HTTPS). Unencrypted web sessions (HTTP) are NOT supported.
- 2.3. If the GUI System Time is not set properly it can cause a situation where the interface results in an immediate timeout when logging in. The solution is to set the time.

3 SNMP

- 3.1. SNMP Service: Going from an ON state to OFF and back ON which is necessary for configuration changes, results in SNMP traps for all down ports and power supplies.

4 RADIUS/TACACS+

- 4.1. Only port 49 is supported for TACACS+ AA.
- 4.2. RADIUS/TACACS+ authentication and authorization are supported for GUI, SSH, and Local Console access, not TELNET access.
- 4.3. Radius Secret/Timeout can be modified based upon a specific IP/port pair. Tacacs Secret/Service can be modified based upon a specific IP/port pair. IP/port pairs cannot be modified only removed, then re-added.
- 4.4. When external RADIUS or TACACS+ is configured as the primary authentication with LOCAL as secondary authentication, the username/password WILL NOT be checked against the LOCAL user database if the external authentication server rejects a GUI login attempt.
- 4.5. When external RADIUS or TACACS+ is configured as the primary authentication with LOCAL as secondary authentication, the username/password WILL be checked against the LOCAL user database if the external authentication server rejects an SSH login attempt.
- 4.6. For Console login, the LOCAL user database is always checked first to avoid being locked out of a box. If RADIUS/TACACS+ is configured as secondary authentication, the request for external authentication will only occur when the LOCAL authentication has failed.

4.7. LOCAL user accounts can only be added/deleted/modified(rights) by logging in using a LOCAL account with User Permissions (i.e., Administrator) LOCAL user accounts cannot be edited by logging in using a RADIUS/TACACS+ account.

4.8. TACACS+ server configuration change does NOT automatically propagate to future authentication processing. The authentication order MUST be reset in order for the server configuration to be applied to future authentication requests. RADIUS server configuration changes DO automatically propagate to future authentication processing.

5 Boot-up

5.1. The status LED on front panel indicates the device is ready several seconds before it is ready to respond to CLI commands.