Datacom Systems Inc.

9 Adler Dr.
East Syracuse, NY 13057
Phone: +1-315-463-9541
Support: www.datacomsystems.com

Release Notes

Firmware for: VS-1012-F, VS-1012-F-1pwr, VS-1112-F, VS-1024-F, VS-1124-F, VS-1212-F, VS-1224-F

Upgrade File Name: Orion. 1.4.20160607.tar.gz
Upgrade Build: Located on production build server.

Compatible Browsers: Goggle Chrome, Microsoft Internet Explorer, Mozilla Firefox

Release Version: 1.4.20160607

Installation Notes (When upgrading from Orion.1.2.4048):

Note 1: Improved password encryption and length. This feature requires the user to change their password after upgrade due to change in encryption mechanisms. Their new password is reset to their [Username]123. If the Username is “Administrator” the password after the upgrade will change to “Administrator123”

Note 2: Configuration backups from previous version of firmware are not supported and should not be used since they will result in device instability and loss of configuration.

Note 3: Copper 10mb is no longer a supported port speed. Any configured 10mb ports will be changed to copper auto negotiate after the upgrade.

Installation Notes (When upgrading from Orion.1.3.20141216 or later):

Note 1: NTP server configurations and Remote Event Log configurations will be reset to their default values

Changes in version 1.4.20160607

1. **Additions**

   GE LB command shows Self-Healing State

   GE PO CO displays on Telnet and SSH sessions

2. **Fixes**

   Fixes user permission issues in GUI caused by RESET TO FACTORY DEFAULTS.

   Fix Sysname does not get written back into product.def file, so that on RE FA DE the current model can be stuffed into the product.ini SysName field.

Know Problems:

Functional:

FB1543 - Unclear error code when issuing a SET LBC STATE command the following error message is displayed: “ERROR - SWITCH LIBRARY”
Should this message appear during the activation of an LBC (SE LB ST "name" AC) the user should first confirm the correctness of any filters applied to the ingress ports.

FB1545 – Filter names are more restrictive that the CLI when the filter is created or edited in the GUI. Only alphanumeric and underscore are allowed in the GUI.

FB2040 - Non alpha-numeric characters not supported in TACACS+ key.

FB 2041 - When creating an IP filter in the GUI, depending on the browser the IP mask fails to give a valid option.

FB2063 - If the tab key is used on the page Authentication and Authorization while you are in pop up window the cursor will tab to fields on the page that are outside the popup window.

FB2141 - ADD NTP SERVER command allows erroneous IP addresses.

FB2175 - RADIUS & TACACS login through SSH fails.

FB2517 - Unrestricted Traffic Flow While Recalculating Hash

Cosmetic:

FB2136 – “REGEN WEB CERTIFICATE “, "ADD NTP SERVER" and "REMOVE NTP SERVER" produce a double echo on subsequent commands after use. The issue is resolved by ending the session and starting a new session.

FB2178 – SHOW PORT ROUTING shows a steering map that is not quite right when placing ports with steering in an LBC. However disabling and enabling the LBC clears this state. Traffic is not affected.

Notes and Limitations:

1 CLI and GUI

1.1. The following characters should not be used for names or descriptions:

1.1.1. Curly brackets (braces) **{ }**
1.1.2. Backslash ****
1.1.3. Pipe **|**
1.1.4. Tilde **~**
1.1.5. Number sign **#**
1.1.6. Grave accent **`**
1.1.7. Quotes **“**
1.1.8. Apostrophe **‘**
1.1.9. Colon **:**

These characters may cause inconsistent displays, or misinterpreted entries.

1.2. GUI supports only encrypted web sessions (HTTPS). Unencrypted web sessions (HTTP) are not supported.

1.3. 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.

2 SNMP

2.1. 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.

3 Load Balancing

3.1. A Port Group configuration change does not automatically propagate to a Load Balancing Configuration. Instead the Load Balancing Group portion of the Load Balancing Configuration must be edited to take into account changes to the Port Group.

3.2. Load Balancing: A port which is not a member of an applied Load Balancing Configuration can be steered to one-or-more of the output ports associated with an applied Load Balancing Configuration. In this case, the data transmitted by the output port(s) will include both the Load Balanced data and the port-steered data. To assure that Load Balance Configuration ports transmit ONLY Load Balanced data, the operator must check-for and eliminate any port-steering that has been applied to the output port(s).

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 Filtering

5.1. The number of filters definitions that can be listed using the SHOW FILTERS command is 128. The number of filters that can be defined is only constrained by the onboard memory which can store thousands of filter definitions.

5.2. A single filter definition can contain up to 64 rules. A rule is a set of one-or-more match conditions for distinct filter types (such as MAC address, IP address, TCP port, UDP port, etc.) which are joined by the "AND" operator. Multiple rules can be joined by the "OR" operator. More than one match condition on a specific filter type requires more than one rule. The filter type match conditions are one of the following: MAC address, IP address, TCP Port, UDP Port, Ether Type, IP Protocol, IPv6 address.

5.3. When defining an exclude filter, the use of a "!" or "NOT" or "DROP" (not operators) syntax must be enclosed within an outer-most set of parenthesis. Only one NOT operator is allowed per filter. It must be used at the top-most level of the filter expression or form. Specifically, the NOT operator MUST be enclosed in its own set of parenthesis. The actual filter that is to be 'NOT'ed, is within its own set of parenthesis. For example, if an IP address INCLUDE filter is defined as (ip.addr == 2.3.4.5), the corresponding EXCLUDE filter must be expressed as (!(ip.addr == 2.3.4.5)) or (NOT(ip.addr == 2.3.4.5)) or (DROP(ip.addr == 2.3.4.5).

5.4. Complex filters that contain a mix of rules enclosed with parenthesis and without parenthesis may be flagged as invalid.

5.5. A maximum of 16 ports can have an egress filter applied on the VS-1224-F, VS-1024-F and VS-1124-F; the number of ports to which a complex multi-rule egress filter can be applied may be less than 16.

6 Port Settings

6.1. SET PORT TYPE – Port Type checking is not enforced for port steering in the CLI; however Port Type connection rules are enforced for port steering in the GUI. Port Type checking allows or restricts connectivity between different ports labeled as Network, Monitor, Active Monitor or Interconnect ports.

7 Port Steering

7.1. Traffic will be dropped in a port steering replication setup when an egress port is oversubscribed and affect the rest of the ports in the setup.

8 Load Balancing

8.1. The number of ingress ports in a load balancing configuration are limited to 16.

9 GUI

9.1. The default user permissions for new features in the GUI are read only. To get the full permissions the Administrator account has to be used to assign privileges.

10 Boot-up

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