

Ethernet Routing Switch 4000 Series Software Release 5.8.1

1. Release Summary

Release Date: 19-May-2015

Purpose: Software patch release to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

“Lockout for failed logon attempts” and “Multiple local RW and RO user accounts” features were introduced with 5.8.0 release (more details can be found in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505).

When upgrading from an earlier release, in order to avoid any issues (please see section 8 Outstanding Issues and section 9 Known Limitations below) caused by these security changes, please default your users name and change the password to be compliant with 5.8.0 password format (more details about password format in 5.8.0 can be found at page 72 in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505).

```
#username RO ro
> enter compliant password
#username RW rw
> enter compliant password
```

3. Platforms Supported

Ethernet Routing Switch 4800 Series Only

4. Notes for Upgrade

Please see “Ethernet Routing Switch 4000 Series, Configuration – System, Software Release 5.6” (available at <http://www.avaya.com/support> . Click Products, select Ethernet Routing Switch 4000 Series from the A-Z list, then select Documentation > View All Documents) for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
4000_58001_diag.bin	Diagnostic image	1,934,853
4000_581028.img	Agent code image	10,733,228
4000_581029s.img	Agent code image (Secure / SSH)	11,006,916

5. Version of Previous Release

Software Version 5.8.0.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM).

7. Changes in This Release

7.1. New Features in This Release

None.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

wi01178902 - Delays in stack port traffic switch between guest VLAN and data VLAN for dhcp-snooping or mac-max settings

wi01178898 – With ADAC configured on the switch and one of the MLT ports as up-link port, upon reboot of the stack, the second MLT port was disabled when the stack came back up and the ADAC VLAN membership was removed from that port

wi01206670 - Devices freeze up after connecting a client with IP of VRRP

wi01206882 - No EAPoL Req identity was sent after a port shut/noshut was performed.

wi01185871 - ERS 4800/After upgrading to v5.8 syslog was not properly logging messages

wi01207055 - After entering the CLI command "snmp-server view xxx +1.3.6.*" the CLI became unresponsive and next session failed to perform 'conf t'.

wi01190195 – A SW Exception: Task tCDTMain Type Data Access issue was addressed in this release

wi01206593 – An EAP related issue in conjunction with Odyssey (Juniper) supplicant was fixed in this release

wi01190396 – The switch LLDP neighbors did not show the Cisco switch whereas the Cisco switch properly reflected the ERS information

wi01171281 - Unicast EAPoL packets were not properly processed by the switch

wi01192695 - After upgrading to 5.8, a number of intermittent RW access failures via Telnet / EDM occurred

wi01187661 - ERS4850 VLACP/ISIS adjacency bouncing on stacks after upgrading to 5.8

wi01192463 - Stack loosing connectivity on one of its NNI ports took a long time to converge and use the alternate path.

wi01201072 – Intermittent Stack link down or missing stack health errors after reboots

wi01207064 - SPBM & Stacking / ISIS remained disabled on non-base unit after a base unit failure

wi01200286 – A more robust switch behavior when a supplicant in 'authentication state' sends an EAP-start to the authenticator

wi01200345 – After upgrading to 5.8 and deleting the RW username, it was not possible to add it back

wi01190406 - LLDP packets from switch, triggered by fast start, sometimes were missing the network policy TLV

wi01195826 – Could not authenticate EAP clients at times after upgrading to 5.8

wi01205259 – The backdoor password did not work for ERS 4000 series

wi01210985 - The switch is now compliant with the TIA 1057 standard where LLDP - MED specific TLV sets transmission from a network device will only begin after an LLDP-MED device has been detected on that port

wi01208569 - Cascade errors and loss of configuration after upgrading to 5.8

wi01205395 – A password related issue when some 5.8 users were locked out after 90+ days (default), is addressed in this release

wi01194514 - ERS4K MAC table "not aging" issue

8. Outstanding Issues

wi01210690 – The switch cannot be accessed if a user is deleted by ACLI, while the same user is connected via EDM.

wi01211320 - User cannot login through EDM after the warning message regarding password expiration for that user is generated.

wi01210770 – In 5.8 with nonconformity password configuration, the switch cannot be accessed using users configured on 5.7,

wi01206642 – With MHM configured, the show ip dhcp-snooping binding tables do not show entries for NEAP or EAP clients.

9. Known Limitations

wi01205602 - The password aging time and history parameters were defaulted after upgrading to 5.8.0.

10. Documentation Corrections

wi01193323 – A number of EAP related documentation inconsistency between CLI and EDM in 5.7 release notes is now properly addressed

wi01201124 - Password security feature can be disabled on secure images

wi01205608 - The documentation for password aging-time was not up to date in the document NN47205-505_10_01

wi01199039 –The transmit-interval parameter needs to be removed from NN47205-505_10_01_Security.pdf (Configuring Security on Avaya Ethernet Routing Switch 4000 Series)

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: <http://www.avaya.com/support> .

11. Troubleshooting

As good practices of help for troubleshooting various issues, AVAYA recommends:

- configuring the device to use the Simple Network Time Protocol to synchronize the device clock;
- setting a remote logging server to capture all level logs, including informational ones. (#logging remote level informational).

Copyright © 2015 Avaya Inc - All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web at: <http://www.avaya.com/support>.