avaya.com

Ethernet Routing Switch 4800 Series
Software Release 5.11.2

1. Release Summary

Release Date: 23-March-2018
Purpose:

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

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4800 (all models).

4. Notes for Upgrade

Please see "Release Notes for Avaya Ethernet Routing Switch 4000 Series Release 5.11, NN47205-400", available at http://support.avaya.com for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
4000_58003_diag.bin	Diagnostic image	1,934,909
4800_5112013s.img	Agent code image	13,116,268

5. Version of Previous Release

Software Version 5.11.1.

6. Compatibility

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

7. Changes in This Release

New Features in This Release

None.

Old Features Removed From This Release

None.

Problems Resolved in This Release

ERS454800-2835, ERS454800-2836 - ERS4800s running 5.11.x code can't process untagged management I-SID traffic packets if it is received encapsulated by a VOSS 9K or ERS8600.

ERS454800-2820 – Memory leak visible when processing IGMPv3 packets; IGMPv1/v2 not affected

ERS454800-2825 - EAP enabled port allows traffic before switch reconfiguration based on RADIUS assigned VLAN is complete

ERS454800-2807 - When COM+ monitoring tool discovery ARP ingresses management VLAN on a non-base unit port, ERS4800 does not send ARP reply back.

ERS454800-2834 - Unknown chassis type of VSP 8k on ERS 4850 topology table

ERS454800-2837 - Clients are unable to receive IP address from /25 or /26 subnet with DHCP relay configured

ERS454800-2846 - NEAP via Radius authentication delay was not respected when an EAP authentication was still in progress for the same MAC address

ERS454800-2860 - "tCDTMain" exception logged when new unit added to stack

8. Outstanding Issues

None.

9. Known Limitations

None.

10. Documentation Corrections

SHA–2 support for SSL certificates

Support for SHA–1 is deprecated and SHA–2 (SHA-256) is now supported for SSL certificate. The reason is Microsoft Security Advisory 2880823. According to the announcement, on January 1, 2016, trusting Code Singing Certificates generated with a SHA-1 hashing algorithm will be stopped, and on January 1, 2017, trusting SHA–1 generated SSL certificates will be stopped.

Warning:

When upgrading from a release that uses SHA-1 based certificate signature to a release that uses SHA-256 based certificate signature, the old certificate is used with the upgraded software which fails to negotiate SSL sessions because it lacks support for SHA-1.

Starting with 5.9.3, only SHA-256 hash algorithm is supported to compute SSL certificate signature.

The solution to successfully negotiating an SSL session when having a signature hash computed with a deprecated algorithm is to regenerate the SSL certificate using a release that supports SHA-256.

Regenerating the certificate depends on CPU usage and can take from 20 seconds up to 15 minutes and it is important to make sure the regeneration is complete before using the new SSL certificate.

Steps to regenerate the certificate:

After upgrade, regenerate the ssl certificate:

(config)#ssl certificate

2. The SSL certificate is regenerated in the background. You must wait till the regeneration is fully complete, as it may take several minutes. How to make sure that the regeneration has finished:

```
(config)#show ssl
[..]
Generation in progress: Yes
[..]

(config)#show ssl
[..]
Generation in progress: No
[..]
```

3. Once the 'show ssl' command displays **'Generation in progress: No',** reset the ssl server for the new certificate to be used:

(config)#ssl reset

Steps to verify if the SSL certificate needs to be regenerated

Before upgrading, verify in the browser that the current certificate signature algorithm is SHA-1. If upgrading to a version starting with 5.9.3, after upgrade the certificate will have to be regenerated so that SHA-256 is used in the certificate signature.

If the old certificate hash is SHA-1 based and the new software supports only SHA-256, the SSL handshake will fail and the certificate details cannot be displayed in the browser.

Examples:

When using **Mozilla Firefox** browser, in the browser address bar, click on the padlock and then on "**More Information**":

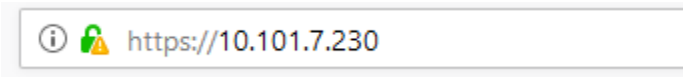

Figure 1

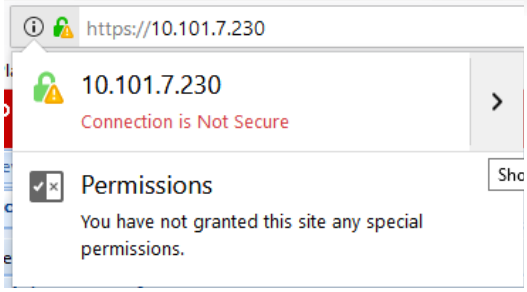

Figure 2

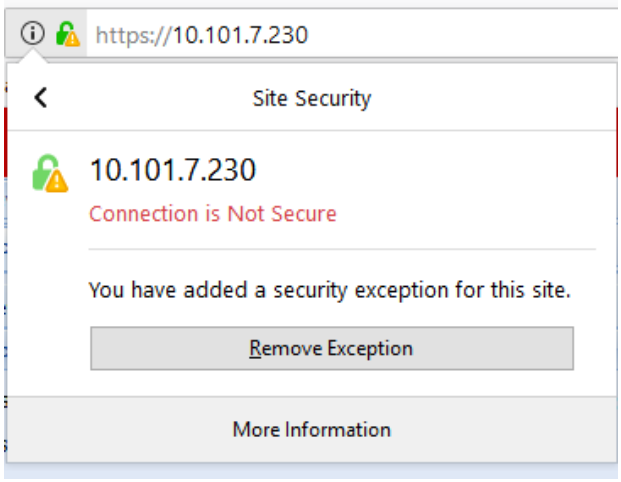

Figure 3

In the **Security** section click on **View Certificate.** Go to the **Details** tab, as shown in Figure 5. Here we can verify the hash algorithm used for the SSL certificate signature.

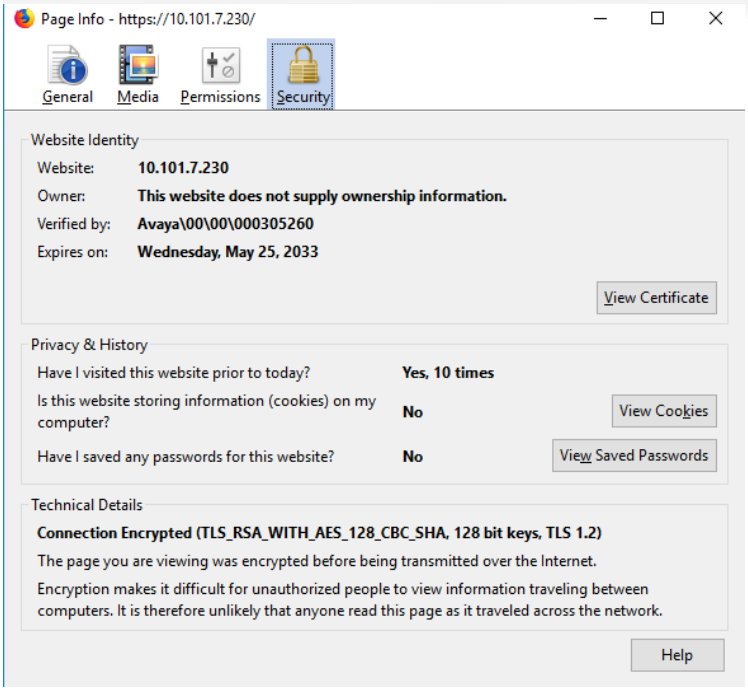

Figure 4

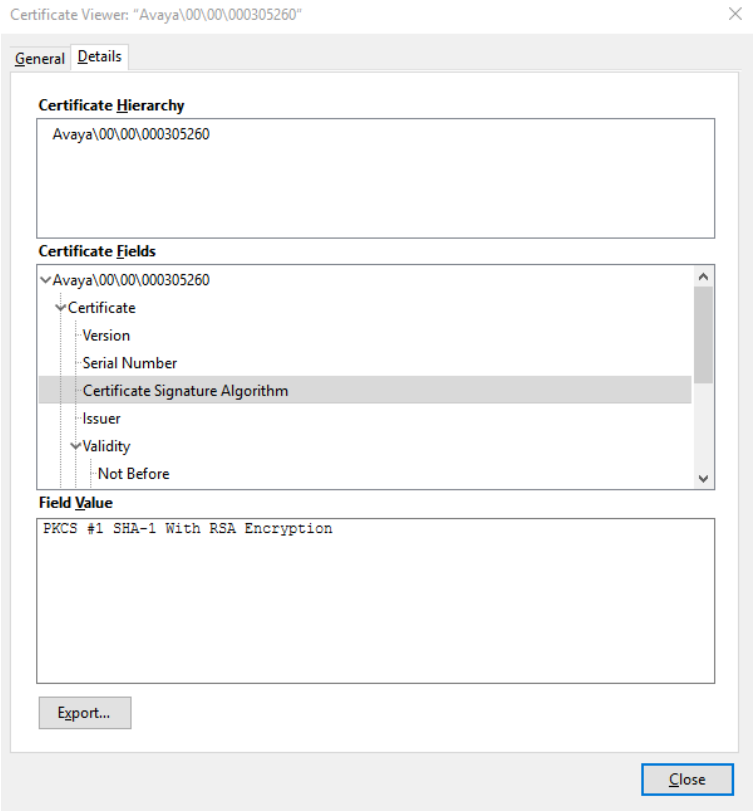

Figure 5 Firefox SSL certificate signature hash algorithm

When using **Internet Explorer** browser, the certificate signature hash algorithm can be viewed by clicking the padlock in the browser address bar and clicking "**View Certificates**" button.

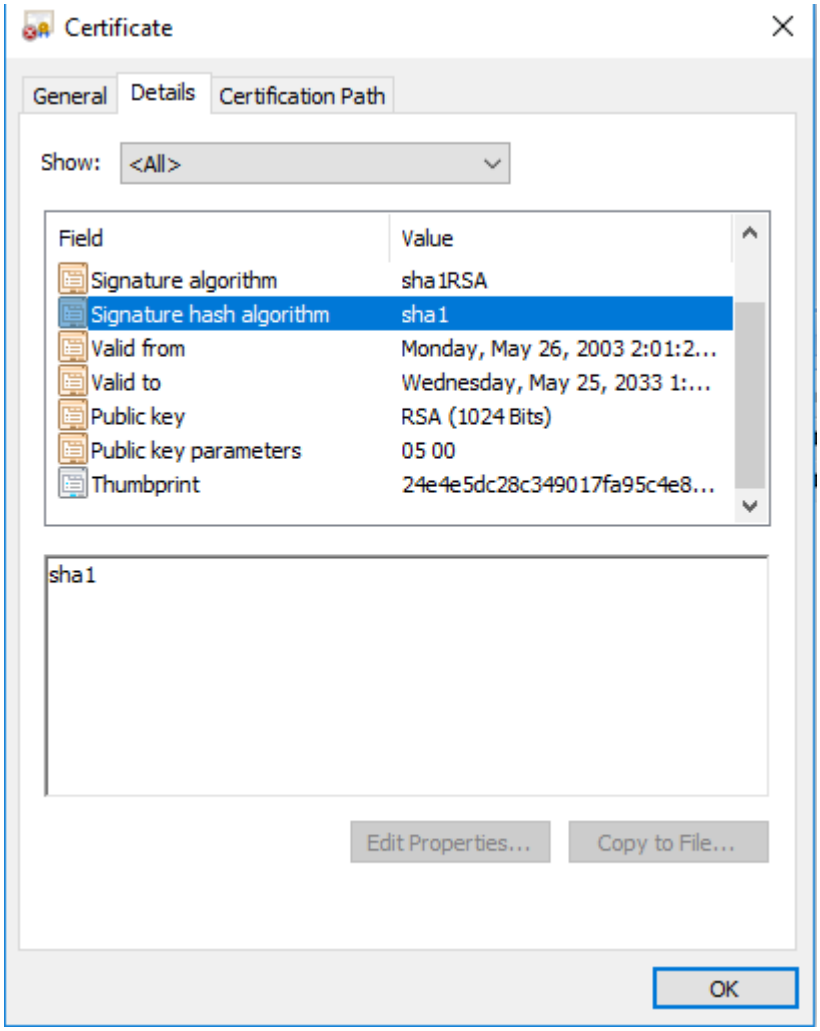

Figure 6 IE SSL certificate signature hash algorithm

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).

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.