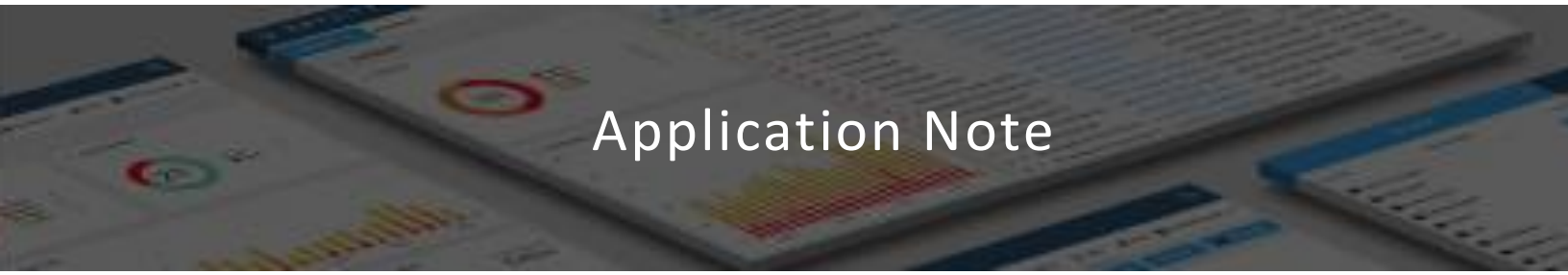
ENTUITY
NETWORK ANALYTICS



Application Note

Excluding SSL Cert Output for Cisco Devices

ENA Configuration Monitor

April 4, 2019

Pete Bartz - Entuity

Table of Contents

1 Overview

Configuration Monitor facilities in ENA are an efficient method to retrieve and compare configurations. In the case of Cisco devices that are configured to authenticate using SSH, there is an issue where the SSL certificate is displayed as output from the “Show running-configuration” command.

When running the comparable “Show startup-configuration” command the SSL details are not included which leads to an automatic discrepancy between running and startup.

The SSL details that are included in the running configuration have minimal value when reviewing or restoring configurations and because of this, it’s reasonable to exclude them.

This Application note provides methods to both ignore the differences when comparing the running and startup configurations and remove redundant SSL cert detail that is included in the show commands by default.

2 Ignore the SSL Cert details using ENA Exclude file

By default, the running configuration output will include details about the SSL cert. An example is shown below.

```
crypto ca certificate chain TP-self-signed-3276704256
 certificate self-signed 01
  308202AB 30820214 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  5D312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33323736 37303432 3536312A 30280609 2A864886 F70D0109
  02161B41 75737469 6E2D5352 2D30312E 6368616D 706C696E 2E6C6F63 616C301E
  170D3933 30333031 30303031 30305A17 0D323030 31303130 30303030 305A305D
  312F302D 06035504 03132649 4F532D53 656C662D 5369676E 65642D43 65727469
  66696361 74652D33 32373637 30343235 36312A30 2806092A 864886F7 0D010902
  161B4175 7374696E 2D53522D 30312E63 68616D70 6C696E2E 6C6F6361 6C30819F
  300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100C307 1F318B65
  EEBEE50F 21AA6B88 31F415F9 5D1866DD CD749731 50BF1240 E6A805B6 E19E0BB6
  98471AE9 95ADC3DE 8097752F D1F09C97 5355A42D F43FF379 0D17FE2C B64593F1
  E87961B4 87B33099 E9667217 B481D32C BBEBFA0E 4887E105 AC0711BA E03AB1CA
  FCB2F354 844115E7 788DF3EE 2BB6934C 0426E664 DC3807F7 6E990203 010001A3
  7B307930 0F060355 1D130101 FF040530 030101FF 30260603 551D1104 1F301D82
  1B417573 74696E2D 53522D30 312E6368 616D706C 696E2E6C 6F63616C 301F0603
  551D2304 18301680 1483520C 441863AF 9D40CDED 4D49011C E9220D95 EE301D06
  03551D0E 04160414 83520C44 1863AF9D 40CDED4D 49011CE9 220D95EE 300D0609
  2A864886 F70D0101 04050003 8181005B 84EAE5E2 AB2D72F6 BFB84E12 9DD4A0B8
  C46D4DC3 BC586C0D 9348DFA1 BD94EAE3 FE2FBF17 F2EADE89 D9B19FC5 5FF8DF13
  8ED9D860 968C3416 0ECA38A4 6461FE17 8B8C057F CF8348F5 90BCB7F2 E0120FD2
  B0F2153B 61C91A28 835E8141 8345CB1F 52A5AA81 760DEDC7 D350B4DC 7BC683C4
  763E23FE 0B26C6F5 0A1B3E45 56CA9A
  quit
!
```

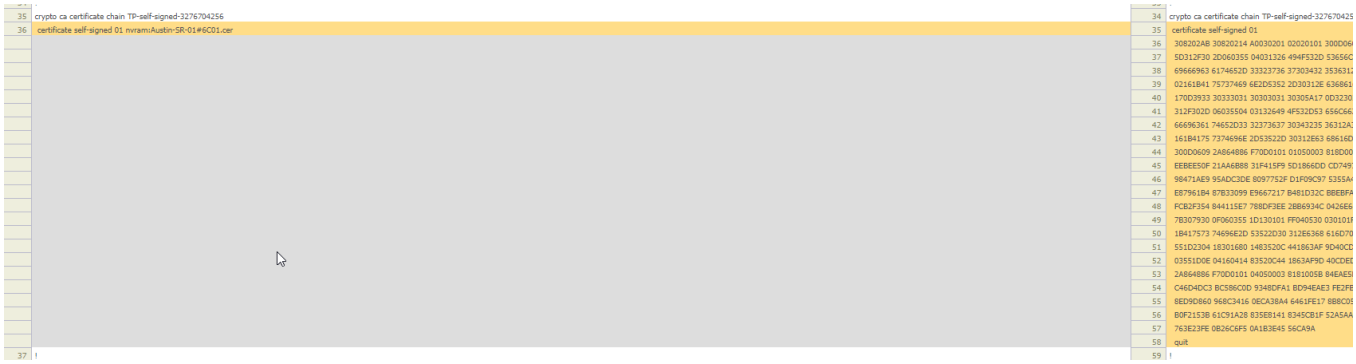
This will generate an ENA event highlighting that the running and startup configurations are different. As this is misleading, creating a rule in the Exclude files is an effective method to ignore this pattern. The following pattern can be added to the Exclude file to ignore this difference.

```
#Ignore self-signed certificate
.*[A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-
Fa-f0-9].*
.*quit
.*certificate self-signed.*
```

This should effectively inhibit the generation of a “CM Unsaved Configuration” incident for this condition.

3 Exclude the display of SSL Cert detail from the show running output.

The addition of the exclude rule defined above will inhibit the generation of an EMS incident but you will continue to see the SSL cert details in the running configuration and when comparing the start and running configurations, the difference will be highlighted as shown below.



This is an annoyance and can be corrected by making a change to the configuration retrieval steps.

The Cisco show command supports the use of exclude logic (similar to a grep command). Modifying the “show running-configuration” command can remove the SSL cert detail. Below is an example highlighting the certificate details.

Standard “show running-configuration” command

```
---clipped---
!
crypto pki trustpoint TP-self-signed-3276704256
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3276704256
 revocation-check none
 rsakeypair TP-self-signed-3276704256
!
!
crypto ca certificate chain TP-self-signed-3276704256
 certificate self-signed 01
  308202AB 30820214 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  5D312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
---clipped---
  B0F2153B 61C91A28 835E8141 8345CB1F 52A5AA81 760DEDC7 D350B4DC 7BC683C4
  763E23FE 0B26C6F5 0A1B3E45 56CA9A
```

```
  quit
!
!
no file verify auto
```

The following change to the command can be used to exclude the certificate details.

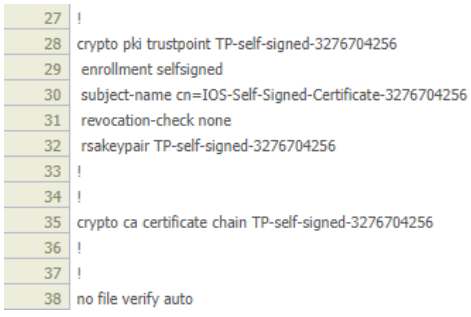
Modified "Show running-configuration" command

show running-configuration | exclude .*[A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9].* | .*certificate self-signed.* | .*quit.*

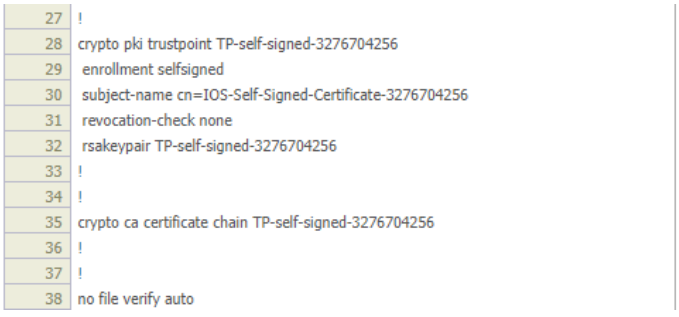
---Output---

```
!
crypto pki trustpoint TP-self-signed-3276704256
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3276704256
 revocation-check none
 rsakeypair TP-self-signed-3276704256
!
!
crypto ca certificate chain TP-self-signed-3276704256
!
!
no file verify auto
```

Applying the same exclude to the "show startup-configuration" command will provide a reasonable comparison in the UI.



```
27 !
28 crypto pki trustpoint TP-self-signed-3276704256
29  enrollment selfsigned
30  subject-name cn=IOS-Self-Signed-Certificate-3276704256
31  revocation-check none
32  rsakeypair TP-self-signed-3276704256
33 !
34 !
35 crypto ca certificate chain TP-self-signed-3276704256
36 !
37 !
38 no file verify auto
```



```
27 !
28 crypto pki trustpoint TP-self-signed-3276704256
29  enrollment selfsigned
30  subject-name cn=IOS-Self-Signed-Certificate-3276704256
31  revocation-check none
32  rsakeypair TP-self-signed-3276704256
33 !
34 !
35 crypto ca certificate chain TP-self-signed-3276704256
36 !
37 !
38 no file verify auto
```

To implement this change, the configuration retrieval step needs to be modified. Note that you will need to use the SSH retrieval method as the Cisco "copy" command doesn't allow the use of exclude logic.

The Cisco SSH configuration retrieval step is not provided as a standard step but is available from support and provided in a separate Application Note.

Modify the step to include a new variable with the proper pattern to exclude. A portion of the original step is shown below.

```
expect.with
{
  // Script restricted to use with Cisco kit as that's all it been tested against.
  if( vendor.equals("9") )
  {
        // String to match when looking for more prompt used for paging.
        def morePrompt = " --More--";

        // Iterate over show command and destination base file name pairs.
        [ ["show startup-config", "startupconfig"],
     ["show running-config", "runningconfig"] ].each
    {
```

The modified step is shown below.

```
expect.with
{
  // Script restricted to use with Cisco kit as that's all it been tested against.
  if( vendor.equals("9") )
  {
        // String to match when looking for more prompt used for paging.
        def morePrompt = " --More--";

        // String to define exclude pattern to remove the ssh key from the show output.
        def excludePattern = " | exclude .*[A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9][A-Fa-f0-9].* | .*certificate self-signed.* | .*quit.*";
```

```
        // Iterate over show command and destination base file name pairs.
        [ ["show startup-config" + excludePattern, "startupconfig"],
      ["show running-config" + excludePattern, "runningconfig"] ].each
    {
```

Save the updated configuration step and apply it to the required devices.