|  |
| --- |
| Customer Acceptance Test Plan (CATP) |
| SAOS 10.7.1 – Part 1 Commissioning and Basic Configuration |
| **Ciena** |
| **5/18/2022** |

### LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PRINTING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

ALL THIRD PARTY TOOLS AND EQUIPMENT REFERENCED IN THIS DOCUMENT ARE FOR ILLUSTRATIVE PURPOSES ONLY. CIENA’S REFERENCE TO OR USE OF SUCH THIRD PARTY TOOLS OR EQUIPMENT HEREIN DOES NOT REPRESENT ANY AFFILIATION WITH THE OWNER OF SUCH TOOLS OR EQUIPMENT OR AN ENDORSEMENT OF SUCH TOOLS OR EQUIPMENT BY CIENA. YOU HAVE NO OBLIGATION TO USE SUCH THIRD PARTY TOOLS OR EQUIPMENT, AND AGREE TO ACCEPT SOLE RESPONSIBILITY SHOULD YOU DECIDE TO USE SUCH THIRD PARTY TOOLS. CIENA DISCLAIMS ALL WARRANTIES AND LIABILITIES AND IS NOT RESPONSIBLE FOR YOUR USE OF SUCH THIRD PARTY TOOLS OR EQUIPMENT.

#### Copyright© 2021 Ciena® Corporation. All Rights Reserved.

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

#### Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

For office locations and phone numbers, please visit the Ciena web site at [www.ciena.com](http://www.ciena.com/).

## Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DATE** | **Issue** | **DESCRIPTION** | **Author/Contributor** | **Reviewer** |
| 10-25-2019 | 0.1 | CATP DRAFT for SAOS 10.3 | Chitvan Shah/Suniti Garg/Abhishek Jain/  /Kevin Estabrooks /Tina Wu | Approver: Nathan Sivanathan |
| 02-24-2020 | 0.2 | CATP completed for SAOS  10.4 (The new features introduced in 10.4 release has been highlighted with  Turquoise colour) | Chitvan Shah/Suniti Garg/Abhishek Jain/  /Kevin Estabrooks /Tina Wu /Seckin Varol/ Yasir Tanveer | Approver: Nathan Sivanathan |
| 09-28-2020 | 0.3 | CATP completed for SAOS  10.5 (new features  introduced in 10.5) | Abhishek Jain/Manoj Sharma/Seckin Varol/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath  Rajamannar/Tina Wu | Approver: Nathan Sivanathan |
| 09-29-2020 | Draft SAOS 10.5 | CATP for SAOS 10.5  edited with comments received from internal review. | Abhishek Jain/Manoj Sharma/Seckin Varol/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath  Rajamannar/Tina Wu | Approver: Nathan Sivanathan |
| 11-17-  2020 | Draft SAOS 10.5 | Edited outdated errors from draft CATP 10.5. Future review necessary. | Abhishek Jain/Manoj Sharma/Seckin Varol/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath  Rajamannar/Tina Wu | Approver: Nathan Sivanathan |
| 12-20-  2020 | Draft SAOS 10.5.1 | Added additional testcases for SAOS 10.5.1 | Abhishek Jain/Manoj Sharma/Jagan Kumar Veluchamy/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath  Rajamannar/Tina Wu | Approver: Nathan Sivanathan |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12-21-  2020 | Final SAOS 10.5.1 | Reviewed and made edits according to review feedback. | Abhishek Jain/Manoj Sharma/Jagan Kumar Veluchamy/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath  Rajamannar/Tina Wu | Approver : Nathan Sivanathan |
| 6-28-2021 | Final SAOS 10.6 | Reviewed and made edits according to review feedback. | AbhishekJain/Manoj Sharma/JaganKumar Veluchamy/Jean-Luc Dupont/Kevin Estabrooks/Vineeth/ Jagannath Rajamannar/Tina  Wu/Izack Vail | Approver : Nathan Sivanathan |
| 9-9-2021 | Draft SAOS 10.6.1 | Added additional  testcases for SAOS 10.6.1 | Kevin Estabrooks/Soukaina Zahidi/Tina Wu/Izack Vail | Approver: Nathan Sivanathan |
| 12-3-2021 | Final SAOS 10.7.0 | Reviewed and made edits according to review feedback. | AbhishekJain/Manoj Sharma/JaganKumar Veluchamy/Jean-Luc Dupont/Kevin Estabrooks/Vineeth  /Jagannath Rajamannar/Tina  Wu/Hicham/Izack Vail | Approver : Nathan Sivanathan |
| 5-18-2022 | Draft SAOS 10.7.1 | Added additional testcases for SAOS 10.7.1 | Abhishek Jain/Manoj Sharma/Jagan Kumar Veluchamy/Kevin Estabrooks/Vineeth/Hars h/Jagannath Rajamannar/Tina Wu/Soukaina Zahidi/Izack  Vail | Approver: Nathan Sivanathan |

**Table of Contents**

1. [Overview 13](#_bookmark0)
2. [Software Installation and Initial Configuration 19](#_bookmark1)
   1. [Software Installation 19](#_bookmark2)
      1. [Access CLI interface 19](#_bookmark3)
      2. [ZTP 21](#_bookmark4)
      3. [SZTP 21](#_bookmark5)
      4. [Verify Re-Install or Upgrade Software 23](#_bookmark6)
      5. [Verify Manual network-based installation 25](#_bookmark7)
      6. [Verify USB-based installation of SAOS 10.x 26](#_bookmark8)
      7. [Verify NTP or verify the date and time 28](#_bookmark9)
      8. [Configuration – Show running 31](#_bookmark10)
      9. [Applying license – Primary License Server 32](#_bookmark11)
      10. [License Server – primary and backup 34](#_bookmark12)
      11. [User Configurable Reg-Id 36](#_bookmark13)
      12. [Manage Active CLI sessions 37](#_bookmark14)
      13. [Reset to factory default 39](#_bookmark15)
   2. [Initial Access and Basic Configuration 40](#_bookmark16)
      1. [Verify System Power Cycle will maintain the configuration 40](#_bookmark17)
      2. [Verify SAOS 10.x software version 41](#_bookmark18)
      3. [SNMP Setup – Through Netconf/YANG 42](#_bookmark19)
      4. [SNMP Configuration - CLI 43](#_bookmark20)
      5. [SNMP v2c Trap Configuration 45](#_bookmark21)
      6. [SNMP v2c Inform Configuration 46](#_bookmark22)
      7. [SNMP v3 Get Configuration 48](#_bookmark23)
      8. [SNMP v3 Trap Configuration 49](#_bookmark24)
      9. [SNMP v3 Inform Configuration 51](#_bookmark25)
      10. [Create New User Account 53](#_bookmark26)
      11. [Validate NACM 53](#_bookmark27)
      12. [Management - Source IP 55](#_bookmark28)
      13. [Syslog Setup 56](#_bookmark29)
      14. [TLS profiles 58](#_bookmark30)
      15. [Pkix and TLS- IP host list 59](#_bookmark31)
      16. [Telemetry 61](#_bookmark32)
      17. [RADIUS over TLS configuration 64](#_bookmark33)
      18. [Syslog over TLS configuration 65](#_bookmark34)
      19. [SSH Public Key Authentication 67](#_bookmark35)
      20. [SSH Rekeying Configuration 68](#_bookmark36)
      21. [DNS Client Setup 69](#_bookmark37)
      22. [L3 DHCPv4 Relay Setup 70](#_bookmark38)
      23. [DHCPv6 Client Setup 73](#_bookmark39)
      24. [Static Mgmt IPv6 Setup 75](#_bookmark40)
      25. [Verify Backup 77](#_bookmark41)
      26. [Verify Reset to User Config (RTUC) 79](#_bookmark42)
      27. [Configuration – Golden Configuration 79](#_bookmark43)
      28. [Port Flap Detection 80](#_bookmark44)
      29. [Low Latency Bypass (currently only available on 5162) 82](#_bookmark45)
      30. [Dot1X – Supplicant Setup 82](#_bookmark46)
      31. [Dot1X – Authenticator Setup 84](#_bookmark47)
      32. [Set up LLDP Global Config 85](#_bookmark48)
      33. [Verify show LLDP for a Connected Port 86](#_bookmark49)
      34. [Debugging – Log monitoring 88](#_bookmark50)
      35. [Debugging – Port Mirroring 90](#_bookmark51)
      36. [NETCONF – RPC commands 92](#_bookmark52)
      37. [DHCP Options (Client Identifier & User Class Options) 93](#_bookmark53)
      38. [Built in Trial License 99](#_bookmark54)
      39. [System gNMI Alarm enhancements 101](#_bookmark55)
3. [FRU 104](#_bookmark56)
   1. [FRU – Testcases 104](#_bookmark57)
      1. [FRU – Filler Mismatch Alarm Disable 104](#_bookmark58)
   2. [5171 – FRU 105](#_bookmark59)
      1. [Insertion of a FRU 105](#_bookmark60)
      2. [Enable FRU module using CLI 107](#_bookmark61)
      3. [Licence install - CFP2-DCO plugs 107](#_bookmark62)
      4. [Configure CFP2-DCO ports 109](#_bookmark63)
      5. [5171 Front Temperature Sensor – Early Notification of High Temperature 110](#_bookmark64)
4. [Device Management 113](#_bookmark65)
   1. [WebGUI 113](#_bookmark66)
      1. [WebGUI – Management of Sessions 113](#_bookmark67)
5. [CLI-based Configuration Test Cases 116](#_bookmark68)
   1. [Base Layer 2 Features 116](#_bookmark69)
      1. [Classifiers 117](#_bookmark70)

[Create untagged traffic classifier 118](#_bookmark71)

[Create single tagged traffic classifier 119](#_bookmark72)

[Create double tagged traffic classifier 120](#_bookmark73)

[Delete a Classifier 122](#_bookmark74)

* + 1. [Flow points and forwarding domains 124](#_bookmark75)

[Create a forwarding domain 124](#_bookmark76)

[Delete a forwarding domain 126](#_bookmark77)

[Create a flow point 127](#_bookmark78)

[Delete a flow point 129](#_bookmark79)

* + 1. [LAG Group - Minimum LAG Aggregation Threshold 130](#_bookmark80)
    2. [LAG Group - Minimum LAG Aggregation Threshold 131](#_bookmark81)
    3. [Configuration of EOAM 133](#_bookmark82)
    4. [Layer 2 Control Protocol 134](#_bookmark83)

[Scenario 1: L2CP Handling 135](#_bookmark84)

[Scenario 2: L2PT (Layer 2 Protocol Tunneling) 139](#_bookmark85)

* 1. [Synchronization – SyncE 142](#_bookmark86)
     1. [Synchronous Ethernet 142](#_bookmark87)
  2. [Synchronization – 10MHz/CLK Interface 143](#_bookmark88)
     1. [10MHz/CLK Interface Input 143](#_bookmark89)
     2. [10MHz/CLK Interface Output 144](#_bookmark90)
  3. [Synchronization – G8275.1 147](#_bookmark91)
     1. [Configure Sync Global Parameters 147](#_bookmark92)
     2. [Configure sync PTP global parameters 148](#_bookmark93)
     3. [Configure frequency and phase protection groups 151](#_bookmark94)
     4. [Configure syncE and PTP input references 152](#_bookmark95)
     5. [Add syncE and PTP input references to frequency and phase protection groups 153](#_bookmark96)
     6. [Configure syncE and PTP output references 154](#_bookmark97)
  4. [Synchronization – GNSS and T-GM Support 155](#_bookmark98)
     1. [General Sync Configuration (G.8275.1) 156](#_bookmark99)
     2. [Enable GNSS 158](#_bookmark100)
     3. [Configure G.8275.1 T-GM 160](#_bookmark101)
  5. [Synchronization - Assisted Full Timing Support 162](#_bookmark102)
     1. [Assisted Full Timing Support Configuration 162](#_bookmark103)
  6. [Synchronization – G8275.2 T-GM 163](#_bookmark104)
     1. [Configure G.8275.2 T-GM 163](#_bookmark105)
  7. [Service Activation Test (SAT) 165](#_bookmark106)
     1. [Configuration of Service Activation Test Generator. 165](#_bookmark107)
     2. [Configuration of Service Activation Test Reflector 168](#_bookmark108)
     3. [SAT testing with inner VLAN ID validation 169](#_bookmark109)
     4. [SAT testing with 1:1 LAG on UNI 184](#_bookmark110)
     5. [SAT events query on syslog server 199](#_bookmark111)
     6. [SAT testing with MPLS LDP transport tunnel 201](#_bookmark112)
     7. [Deleting SAT configurations 217](#_bookmark113)
  8. [CFM Service OAM 220](#_bookmark114)
     1. [Delay Measurement Test 220](#_bookmark115)
     2. [Synthetic Loss Measurement Test 227](#_bookmark116)
     3. [Frame Loss Measurement Test 230](#_bookmark117)
     4. [Loopback Test 233](#_bookmark118)
     5. [Linktrace Test 235](#_bookmark119)
     6. [Configure and verify Static\Manual Remote MEP 236](#_bookmark120)
     7. [L2 Loop Detect 243](#_bookmark121)
     8. [Remote MEP – Deletion of dynamically discovered remote MEP 249](#_bookmark122)
     9. [MEP Support on QinQ 251](#_bookmark123)
        1. [Creating Classifier, fp, fd & flow-point transforms (both ingress and egress) 252](#_bookmark124)
        2. [Enabling CFM 253](#_bookmark125)
        3. [Verification 254](#_bookmark126)
  9. [TWAMP 256](#_bookmark127)
     1. [TWAMP Server and Session Reflector 256](#_bookmark128)
  10. [Static MPLS-TP 258](#_bookmark129)
      1. [MPLS-TP Tunnel Configuration 258](#_bookmark130)
      2. [Static MPLS-TP/PW CLI Show Commands 262](#_bookmark131)
      3. [Static MPLS-TP LSP BFD 264](#_bookmark132)

[Configurable BFD session Parameters 265](#_bookmark133)



[5.11.4](#_bookmark133)

* + 1. [LSP BFD CLI Show Commands 266](#_bookmark134)
    2. [MPLS-TP Static Tunnel – LSP BFD – Hardware acceleration 268](#_bookmark135)
  1. [L2VPN 274](#_bookmark136)
     1. [T-LDP 274](#_bookmark137)
     2. [L2VPN configuration 276](#_bookmark138)
     3. [Static L2VPN 278](#_bookmark139)
     4. [HVPLS configuration with PW redundancy 280](#_bookmark140)
     5. [L2VPN OAM 281](#_bookmark141)
     6. [Dynamic PWE with MTU – Ignore MTU Mismatch 282](#_bookmark142)
     7. [Dynamic PWE – Multi-Hop IP BFD 285](#_bookmark143)
     8. [Dynamic PWE – Mac Withdrawal 287](#_bookmark144)
     9. [Dynamic PWE – WTR 288](#_bookmark145)
     10. [Static PWE – Multi-Segmented PWE 291](#_bookmark146)
  2. [FAT PW overview 294](#_bookmark147)
     1. [FAT PW baseline Lab / Hardware infrastructure 294](#_bookmark148)
     2. [FAT PW Configuration 294](#_bookmark149)
     3. [FAT PW Verification & Results 306](#_bookmark150)
  3. [FAT PW Signaling 311](#_bookmark151)
     1. [FAT PW baseline Lab / Hardware infrastructure 311](#_bookmark152)
     2. [FAT PW Configuration 312](#_bookmark153)
     3. [FAT PW Verification & Results 316](#_bookmark154)
  4. [L2VPN CW CC-Type 4 Signaling 320](#_bookmark155)
     1. [CC-TYPE 4 over PW configuration 321](#_bookmark156)
     2. [CC-Type Verification & Results 324](#_bookmark157)
  5. [L2VPN VPLS over BGP-LU supported for 5162, 5170, 5171 326](#_bookmark158)
     1. [L2VPN VPLS over BGP-LU baseline Lab / Hardware infrastructure 326](#_bookmark159)
     2. [Verification & Results 332](#_bookmark160)
  6. [TDM PWE 334](#_bookmark161)
     1. [TDM PWE -DS1/E1 334](#_bookmark162)
     2. [TDM PWE – OC3/STM1 338](#_bookmark163)
  7. [Layer 2 QoS 344](#_bookmark164)
     1. [COS Mapping 344](#_bookmark165)

[Create a frame to COS map 346](#_bookmark166)

[Create a COS to frame map 349](#_bookmark167)

[Add a frame to COS map to a flow point 351](#_bookmark168)

[Add a COS to frame map to a flow point 353](#_bookmark169)

[Test COS mapping with traffic flow 355](#_bookmark170)

* + 1. [Ingress Metering 356](#_bookmark171)

[Create a meter profile 357](#_bookmark172)

[Define bandwidth calculation mode 359](#_bookmark173)

[Attach a meter profile to a flow point 360](#_bookmark174)

[Test ingress metering with traffic 362](#_bookmark175)

[Test payload calculation mode in ingress metering with traffic 363](#_bookmark176)

* + 1. [Hierarchical Ingress Metering 363](#_bookmark177)

[Ingress Metering - QoS Flow and QoS meter profile 364](#_bookmark178)

[Ingress Metering – Parent Flow point Meter 366](#_bookmark179)

[Ingress Metering – QoS Flow only 367](#_bookmark180)

[Hierarchical Ingress Metering – QoS Flow and Parent Meters 368](#_bookmark181)

* + 1. [Assigning CoS to Non-conforming Packets 369](#_bookmark182)
    2. [Egress QoS 374](#_bookmark183)

[Create a scheduler profile 375](#_bookmark184)

[Create a queue group profile 378](#_bookmark185)

[Create a scheduler instance 381](#_bookmark186)

[Create a queue group instance 383](#_bookmark187)

[. 385](#_bookmark188)

[Bind a queue group to a flow point 385](#_bookmark189)

[Bind a queue group to a logical port 386](#_bookmark190)

[Verify EQoS with traffic 389](#_bookmark191)

[Remove EQoS setup 390](#_bookmark192)

[Configure Low Latency Optimization on Egress Queue 5 390](#_bookmark193)

* + 1. [H-EQOS 391](#_bookmark194)
    2. [CoS Treatment of VRF-injected packets 400](#_bookmark195)
  1. [XGS-PON Overview 403](#_bookmark196)
     1. [uOLT Management Configuration 405](#_bookmark197)
     2. [Register ONUs 408](#_bookmark198)
     3. [ONU Configuration 408](#_bookmark199)
     4. [Create SLA Profile 409](#_bookmark200)
     5. [uOLT Data Link Configuration, Networks and PON Connections 411](#_bookmark201)
     6. [Traffic flows to ONUs Via uOLT and Vice versa 415](#_bookmark202)
  2. [XGS-PON OFF Box Solution 415](#_bookmark203)
     1. [8.6.X XGS-PON OFF Box Solution 415](#_bookmark204)

[8.6.x Configuration for uOLT Management 416](#_bookmark205)

[Configuration on 3926/3906 with FRU 417](#_bookmark206)

[uOLT Management Configuration on PON OAM running on 3926 FRU 417](#_bookmark207)

[Register ONUs 420](#_bookmark208)

[ONU Configuration 420](#_bookmark209)

[Create SLA Profile 421](#_bookmark210)

[uOLT Data Link Configuration, Networks and PON Connections 423](#_bookmark211)

* + 1. [6.x XGS-PON OFF Box Solution 427](#_bookmark212)

[6.x Configuration for uOLT Management 427](#_bookmark213)

* 1. [SAOS XGS-PON ONU Enhancements 428](#_bookmark214)
     1. [Ethernet Private Line (EPL) configuration support on the ONU 428](#_bookmark215)

[uOLT Management Configuration on 5170 429](#_bookmark216)

[Register ONUs 431](#_bookmark217)

[ONU Configuration 432](#_bookmark218)

[Create SLA Profile 433](#_bookmark219)

[uOLT Data Link Configuration, Networks and PON Connections 434](#_bookmark220)

* + 1. [Ethernet Virtual Private Line (EVPL) Service configuration support on the ONU 438](#_bookmark221)

[uOLT Management Configuration on 5170 439](#_bookmark222)

[Register ONUs 441](#_bookmark223)

[ONU Configuration 442](#_bookmark224)

[uOLT Data Link Configuration, Networks and PON Connections 443](#_bookmark225)

[NNI interface Configuration 444](#_bookmark226)

[PON Connection Configuration 445](#_bookmark227)

* + 1. [ONU-to-ONU Cross Connect 445](#_bookmark228)

[uOLT Management Configuration on 5170 446](#_bookmark229)

[Register ONUs 448](#_bookmark230)

[ONU Configuration 449](#_bookmark231)

[Create SLA Profile 450](#_bookmark232)

[uOLT Data Link Configuration, Cross connect and PON Connections 451](#_bookmark233)

* + 1. [ONU Provision using registration ID 454](#_bookmark234)
  1. [XGS-PON Residential Service Support 455](#_bookmark235)
     1. [uOLT Management Configuration 456](#_bookmark236)
     2. [ONU and UNI Port Configuration 458](#_bookmark237)
     3. [Create SLA Profile 458](#_bookmark238)
     4. [uOLT Data Link Configuration, Networks and PON Connections 459](#_bookmark239)

[Data Link Configuration 459](#_bookmark240)

[NNI Interface Configuration 460](#_bookmark241)

[PON Connection Configuration 460](#_bookmark242)

* + 1. [Adding Radius Server info on the Authenticator (PON controller): 461](#_bookmark243)

[5.19.5.1 Step 1: 461](#_bookmark244)

[Step 2: 461](#_bookmark245)

* + 1. [Radius Server reachability to Authenticator (PON controller) 462](#_bookmark246)
    2. [DHCP Server reachability to L2 DHCP relay Agent (PON controller) 463](#_bookmark247)
  1. [Multicast 464](#_bookmark248)
     1. [IGMP Snooping 464](#_bookmark249)

 [Dynamic IGMP snooping Config 465](#_bookmark250)

 [Static IGMP Join Config 468](#_bookmark251)

* 1. [FlexE Introduction 470](#_bookmark252)
     1. [Configure a FlexE Client Port 470](#_bookmark253)
     2. [Configure FlexE Network Port 472](#_bookmark254)
     3. [Create a FlexE Group 474](#_bookmark255)
     4. [Create a FlexE Channel 475](#_bookmark256)
     5. [Create a FlexE Cross Connect 477](#_bookmark257)
     6. [L2 FlexE 478](#_bookmark258)

[Layer 2 FlexE Configuration 479](#_bookmark259)

* 1. [Other: ACL, Flood Containment Profile, 480](#_bookmark260)
     1. [Create an access flow 480](#_bookmark261)
     2. [Delete an access flow 481](#_bookmark262)
     3. [IP ACL 482](#_bookmark263)

[Creation of Access Profiles 483](#_bookmark264)

* + 1. [Create a flood containment profile 485](#_bookmark265)
    2. [Delete a flood containment profile 486](#_bookmark266)
  1. [G.8032: Ethernet Ring Protection 487](#_bookmark267)
  2. [Macsec Encryption 491](#_bookmark268)
     1. [Hop By Hop Mode on 3926 491](#_bookmark269)
     2. [End to End Mode on 3926 500](#_bookmark270)
     3. [End-to-end mode on 5171 509](#_bookmark271)
  3. [ETTP loopback 512](#_bookmark272)
  4. [LLDP support to pick remote management address: 516](#_bookmark273)

1. [Appendix A 518](#_bookmark274)
   * 1. [WebGUI – Create IP Interface 518](#_bookmark275)
     2. [WebGUI – Create IS-IS Instance 521](#_bookmark276)
     3. [WebGUI – Enable LDP 524](#_bookmark277)
     4. [WebGUI – Create BGP Instance 528](#_bookmark278)

## Overview

This test plan is meant to guide customers testing the Ciena SAOS 10.x routing switches. This document describes the product features and intended benefits along with the specific features available in SAOS 10.x for customer testing during this Technology Proof of Concept and Trial phase. Most importantly, this document describes the recommended test set up and procedures to ensure a valuable test.

Ciena 5162, is a pizza box hardware which comes with two 100GE ports and 40 10GE SFP+s. Console pin out is the same as other Ciena devices and it can be accessed at serial baud rate of 115200.



Figure (1): Ciena 5162

Ciena 5170, is a pizza box hardware which comes with four 100GE ports and 40 10GE SFP+s. Console pin out is the same as other Ciena devices and it can be accessed at serial baud rate of 115200.

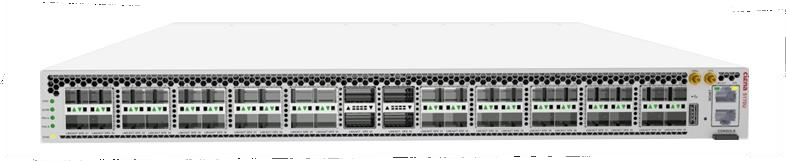


Figure (2): Ciena 5170

In 10.3, new platforms 5171, 3928, and 3926 have been introduced into the 10.x portfolio – depicted below. FRUs are supported on the 5171 as indicated in this document. However, the FRUs in the 3926 are not supported yet in the 10.x stream.

Ciena 5171, is a 2 RU hardware which comes with total of (40) 10GigE ports and (2) 200GigE capacity field replaceable modules (FRU). Different FRU variants supported are - 1 x 100GigE QSFP28 and 1 x 100GigE CFP2 and 2 x 100GigE QSFP28.

Console pin out is the same as other Ciena devices and it can be accessed at serial baud rate of 115200.



Figure (3): Ciena 5171

Ciena 3928, is a pizza box hardware which comes with four 10GE ports and eight 1GE ports. Console pin out is the same as other Ciena devices and it can be accessed at serial baud rate of 9600.



Figure (4): Ciena 3928

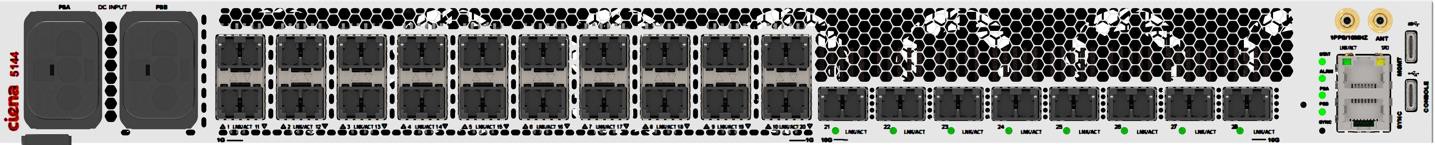
Ciena 3926, is a pizza box hardware which comes with six 10GE and two 1GE ports. Console pin out is the same as other Ciena devices and it can be accessed at serial baud rate of 9600. A newer version of the chassis was also introduced in 10.5 – 170-3926-905 – MACSec ready chassis.



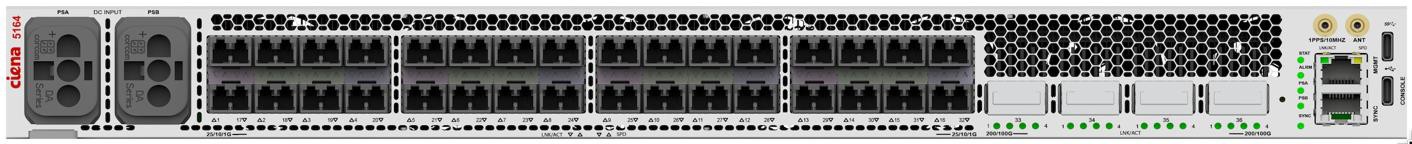
Figure (5): Ciena 3926

In SAOS 10.5, the following platforms are also introduced. The following systems have usb-c connectors for console access (rather than RJ45 connectors on other platforms).

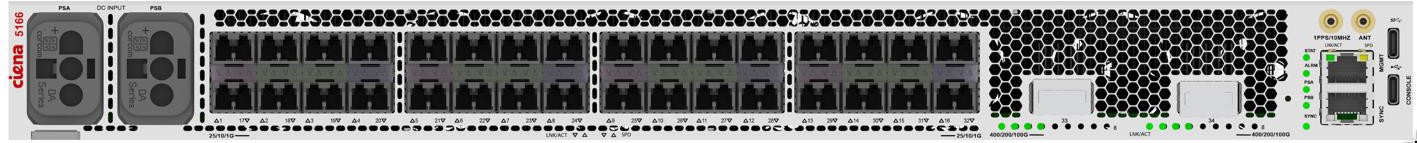
5144 – 20x1G/100M SFP and 8x10G/1G SFP+



5164 – 31x25G/10G/1G and 4x200G/100G ports



5166 – 32x25G/10G/1G and 2x200G/100G (and 400G ready)



In SAOS 10.5.1, the following platforms are introduced. 5130 – 12xSFP28/SFP+, 2xQSFP-28, usbc console port.



3924 – 3x1G/100M SFP, 4x10G sFP+, RFJ45 console port with 9600 baud rate.



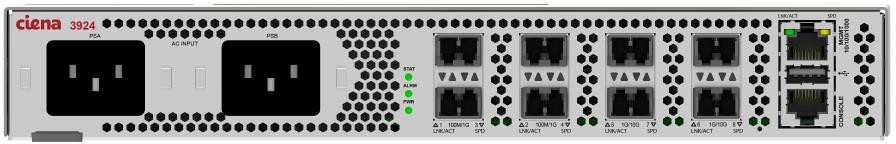
This document includes commissioning and basic configuration of the 10.x platforms. For L3 protocols and services, please refer to **SAOS 10.5.1 – Part 2 L3 Protocols and Services Configuration.**

In SAOS 10.6, the following platforms are also introduced. The following systems have usb-c connectors for console access (rather than RJ45 connectors on other platforms).

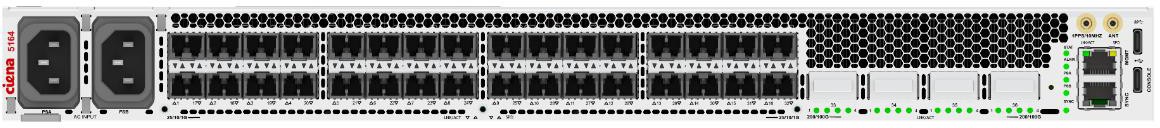
5168 – Q2A based platform, 4x QSFP56/QSFP28 14x SFP28 18x SFP28 CPRI



3924 Dual PS



**5164 Extended Temp**

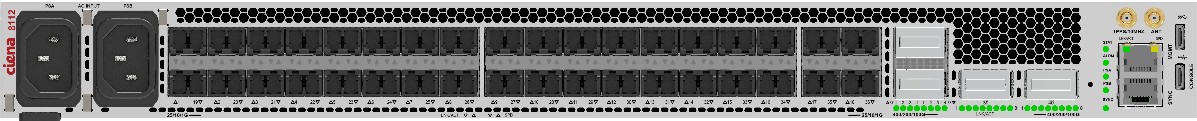


In SAOS 10.6.1, the following platforms are also introduced.

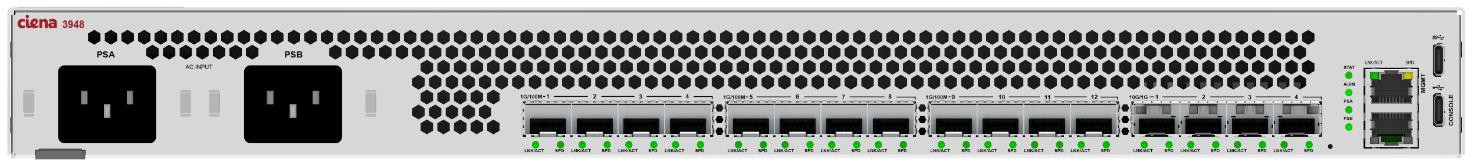
**8110 - 100G PE & Aggregation with WL5 400G ZR**



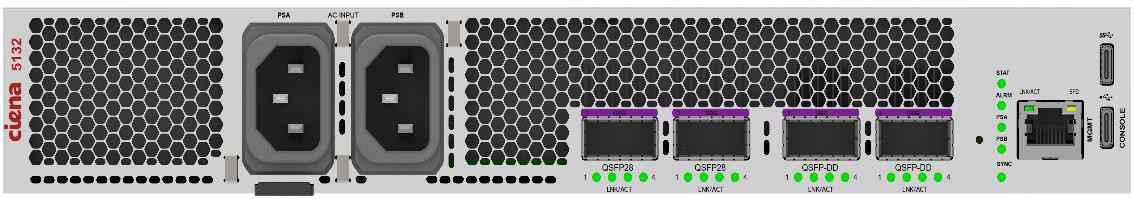
**8112 - 25G/10G PE & Aggregation with WL5 400G ZR**



**3948 10G Aggregation Platform**



**5132 100G Service Access Platform**



In SAOS 10.7.0, the following platforms are also introduced.

**3922 Service Access Platform**



**5131 Weatherproof xHaul Aggregation Router**



**3926 TDM Combo FRU**



In SAOS 10.7.1, the following platforms are also introduced.

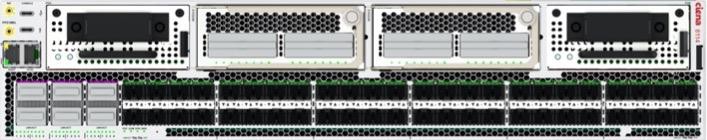
**3926 16x1Gbe FRU**



**5166 CFP2**

A picture containing table  Description automatically generated

**8114**



**Note:**

**This document is created from contributions from many SE&I team members. Although an effort is made to keep similar format for each section/testcase, the formatting of each section and testcases may differ slightly.**

**This CATP is cumulative, it includes all features introduced in previous releases. However, as features are added some of the provisioning commands for existing features may also have changed – due to changes in YANG models. Please refer to prior released CATP if looking for command provisioning in an older release than current CATP. All new/updated testcases are highlighted, please refer Table of Content as reference any updated/new testcases.**

## Software Installation and Initial Configuration

#### Software Installation

###### Access CLI interface

***Objective:***

This test case verifies that the node with SAOS 10.x is reachable from the network for IP management, and to open the CLI for manual CLI-based configuration of SAOS 10.x box.

***Procedure:***

 Login to system through console port. Provision a static IP or check if any DHCP IP has been assigned to local management interface mgmtbr0.

#disable DHCP

dhcp-client client mgmtbr0 admin-enable false

#setup static IP for mgmtbr0

oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20

#Setup static route to default gateway

rib vrf default ipv4 10.0.0.0/8 next-hop x.x.x.x description "default gw"

* Display the IP interfaces.

show ip interfaces brief

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

* + Replace x.x.x.x with IP address of the node.
  + username: diag password: ciena123
  + ~~a “-p 830” parameter for port 830 is only needed for SAOS 10.2 or earlier.~~
  + You will be logged in to the CLI
  + You can now access the configuration interface with typing
    - config

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify Re-Install or Upgrade Software

***Objective:***

Objective is to verify downloading, installation, and activation of software.

***Procedure:***

* Load installation is through ONIE – Open Network Install Environment
* After initial installation of a SAOS load on a box, you should be able to upgrade to another load without need to go back to ONIE.
* \*Following the example below and enter the following command to download the build

from user’s own URL – please note the URL below is for reference only:

software download url [http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml) [0096.yml](http://x.x.x.x/valimar-snapshot/manifest/saos-10-05-01-0096.yml)

* After the a few minutes, the build should have downloaded successfully. Execute a “show software” to check the download status.
* Once the build has downloaded successfully, execute the command install to install the software.

software install package saos-10-05-01-0096 defer-activation

* \*Once installation is complete, activate the load to complete the upgrade.

software activate package saos-10-05-01-0096

* After the a few minutes, the build should have been activated successfully. Execute a

“show software” to check the status. You should see something like this:

5144-009> show software

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| +  | | Name | | | SOFTWARE STATE  Value | +  | | | |
| +  | | Current operation | +  | | idle | +  | | | |
| |  |  |  |  +  |  |  |  |  | | RPC Status  Running package version Package build info Active bootchain  Components: BIOS image  BOOT FPGA image ONIE image  cn\_alarm\_1 | |  |  |  |  +  |  |  |  |  | | idle  saos-10-05-01-0096  Wed Dec 02 03:16:15 2020  01-05-01-0096  0017  00.00.2a Ciena\_2019.02.01-0040  01-05-01-0096 | autouser | onxvpnjk23 | |  |  |  |  +  |  |  |  |  | |
| | | cn\_central-logger\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cfm\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_cnfp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_collectd\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dataplane\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcp-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dhcpl3relay\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dns\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_dot1x\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_eoam\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_erps\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_feds\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_hal\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ipservices\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lacp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_lldp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ntp\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pkix\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_pon-ctrl\_1 | | | 01-05-01-0096 |  |  | | |
| | | cn\_ppm\_1 | | | 01-05-01-0096 |  |  | | |

| cn\_rstp\_1 | 01-05-01-0096 |

| cn\_sat\_1 | 01-05-01-0096 |

| cn\_snmp-agent\_1 | 01-05-01-0096 |

| cn\_storage\_1 | 01-05-01-0096 |

| cn\_svcdirectory\_1 | 01-05-01-0096 |

| cn\_sync-hal\_1 | 01-05-01-0096 |

| cn\_sync\_1 | 01-05-01-0096 |

| cn\_system\_1 | 01-05-01-0096 |

| cn\_tdm\_1 | 01-05-01-0096 |

| cn\_telemetry\_1 | 01-05-01-0096 |

| cn\_twamp\_1 | 01-05-01-0096 |

| cn\_ui\_1 | 01-05-01-0096 |

| cn\_val-gui\_1 | 01-05-01-0096 |

| cn\_ztp\_1 | 01-05-01-0096 |

| xg\_xgrade-agent\_1 | 01-05-01-0096 |

+ + +

| Available packages: | |

**| saos-10-05-01-0096 | activated** |

+ + +

\*can combine the steps and use “software install” without the defer-activation parameter. “software install” will download, install and activate the load on the system in one step.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify Manual network-based installation

***Objective:***

Objective is to install SAOS 10.x on a system, using the manual network-based installation.

***Procedure:***

* Login to system console port.
* When ONIE comes up it will try to find the resource for ZTP. If you want to specify the location of the installer file manually, which is different from what it might fetch from network installer, you should stop it:

ONIE:/ # onie-discovery-stop

* Then proceed with the manual installation from the installer file from http, tftp or ftp server.

ONIE:/ # onie-nos-install <http://x.x.x.x/installer.bin> ONIE:/ # onie-nos-install tftp://x.x.x.x/installer.bin ONIE:/ # onie-nos-install ftp://x.x.x.x/installer.bin

Replace x.x.x.x with IP address or the URL of where the image is residing. Here is an example:

ONIE:/ # onie-nos-install <http://x.x.x.x/valimar-> snapshot/17-12-00-0141/meta-onie-installer-dnx/meta\_01-00- 00-0181-core.bin

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify USB-based installation of SAOS 10.x

***Objective:***

Objective is to install SAOS 10.x on a system using USB-based method.

***Procedure:***

* Ensure that the format of your USB stick is FAT32 formatted.
* Ensure that the image you want is on the USB stick
* Ensure that the image is named “**onie-installer**”. This is important. Currently, the load name cannot be named anything else.
* Start the node if it is the first time it is being powered up, or follow the following steps otherwise
* Login to UI container using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

When ONIE comes up it will try to find the resource for ZTP. Wait for the installation to complete from here.

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Verify NTP or verify the date and time

***Objective:***

Setting date and time are required before application of licenses. Set NTP or date for Ciena SAOS 10.x using Linux commands. Proper data and time setup are required for license application.

***CLI NTP Procedure:***

* Establish a ssh connection to ValCLI

ssh [diag@X.X.X.X](mailto:diag@X.X.X.X)

password: ciena123

* Send the following config command
  + config

system ntp associations remote-ntp-server server-entry 10.33.80.21 admin-state enabled

* Check the NTP State with the following command
  + show ntp client
* The output would be something like:

+---------- NTP CLIENT STATE +

| Name | Value |

+ + +

| Admin State | enabled |

| Mode | polling |

| Polling Min Interval | 16 |

| Polling Max Interval | 16 |

| Auth Admin State | disabled |

| Synchronized | True |

| Delay | 62.161 |

| Offset | 0.006 |

| Jitter | 0.017 |

| Drift (PPM) | -4.485 |

+ + +

+--------- NTP CONFIGURED SERVERS +

| Address | Auth Key ID | Admin State |

+ + + +

| 10.33.80.21 | | enabled |

+ + + +

+ NTP OPER SERVERS

+

| Address | Auth Key ID | Server State | Server Condition | Auth State | Offset |

+ + + + +

+ +

| 10.33.80.21 | | reach | syspeer | none

| 0.006 |

+ + + + +

+ +

***Date & Time Set Procedure:***

* Login to UI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Enter the following command to change the date and time on the system. This will only work if NTP is disabled:

config

system set clock 2018-11-03T18:39:00Z

* Show the system time:

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-03 18:39:03 UTC |

* To enable NTP, the manually set clock will be overwritten.

config

system ntp admin-state enabled

5162-002> show clock

+ System Clock +

| Name | Value |

+ + +

| Current Time | 2018-11-08 13:22:28 UTC |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configuration – Show running

***Objective:***

Objective is to display the show running command

***Procedure:***

* On Valimar cli, display the configuration by issuing following command.
  + show running
* A list of configuration information is displayed in JSON-like format.
* The user can also list the provisioning information per feature basis. To do that, we use the following command to display the sections of the provisioning we can display:
  + show running section ?

5162-003> show running section <TAB>

ciena-bw-calculation-mode:bw-calculation-mode ciena-mef-fd:fds ciena-sync:sync

ciena-cfm:cfm-global-config ciena-mef-fp:fps ciena-tdm-global:tdm-global ciena-dhcp:dhcp-client ciena-mef-frame-to-cos-map:frame-to-cos-maps ciena-tls-service-

profile:tls-service-profiles

ciena-dhcpv6-client:dhcpv6-client ciena-mef-logical-port:logical-ports ciena-tls:hello-params ciena-eoam:eoam-global-config-status ciena-mef-mac-management:mac-management ciena-vrf:vrf

ciena-ieee-lag:agg-global ciena-mef-pfg-profile:pfg-profiles ciena-ztp:ztp ciena-ieee-lldp:lldp-global-config ciena-mpls:mpls ietf-alarms:alarms

ciena-ieee-rstp:rstp ciena-packet-ptp:ptps ietf-netconf-acm:nacm

ciena-isis:isis ciena-packet-xcvr:xcvrs mef-cfm:default-md-levels ciena-itut-g8032-draft:g8032-rings ciena-pkix:pkix openconfig-interfaces:interfaces

ciena-licensing:license-management-config ciena-ppm:ppm openconfig-platform:components

ciena-management-plane:management-plane ciena-rib:rib openconfig-system:system

ciena-mef-classifier:classifiers ciena-sat:sat openconfig-telemetry:telemetry- system

ciena-mef-cos-to-frame-map:cos-to-frame-maps ciena-sr:segment-routing

ciena-mef-egress-qos:egress-qos ciena-subsystem-resource:subsystems

* As an example, display the isis section of the provisioning file.
* show running section ciena-isis:isis

5162-003> show running section ciena-isis:isis ciena-isis:isis

instance

tag Section3

dynamic-hostname True net

49.FAFA.0101.8110.2162.00

level-type level-1 proto-ipv4

redistribute protocol

name static level level-1

fast-reroute level

level-type level-1 lfa

per-prefix-enable True ti-lfa

per-prefix-enable True

level

level-type level-2 lfa

per-prefix-enable True ti-lfa

per-prefix-enable True

interfaces interface

name if5

interface-type point-to-point interface

name if10

interface-type point-to-point interface

name if23

interface-type point-to-point interface

name lb1

interface-type point-to-point mpls-te

router-id 10.181.102.162 level-type level-1

cspf-flag True segment-routing

enabled True srgb

lower-bound 16000

upper-bound 23999

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Applying license – Primary License Server

***Objective:***

Note that the data and time set is required for the application of the license. This step is to apply license to the installed SAOS 10.x software. This will activate the features and ports will be controlled by SAOS 10.x.

***Procedure:***

* Pick one of the lab San Jose or lab Ottawa servers
* config

# license-management-config license-server-config 10.33.80.94

or

# license-management-config license-server-config 10.182.66.137 # exit

# exit

* Confirm the registration and license management state
* show license

You should see an output similar to following

+ License Management State +

| Name | Value |

+ + +

| License-server-state: | |

| Ciena-licensing:server-port | 7071 |

| Hostname | 10.182.66.137 |

| Server-oper-state | enabled |

| License-client-state: | |

|  |  |  |  |
| --- | --- | --- | --- |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Sync | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SYNC-P|p=SAOS SYNCHRONIZATION SOFTWARE LICENSE | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 13 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-Security | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162SEC-P|p=SAOS SECURITY SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 11 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-MPLS | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162MPLS-P|p=SAOS MPLS SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 9 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | License-feature: | | | | |
| | | Source | | served | | |
| | | Feature-name | | SAOS-BaseOS\_AdvEth\_OAM | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162EO-P|p=SAOS BASE OS, ADVANCED ETHERNET & OAM SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 7 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | License-feature:  Source | |  | served | |  | |
| | | Feature-name | | SAOS-Adv\_100G | | |
| | | Version | | 1.0 | | |
| | | Description | | lt=perpetual|pn=S75-LIC-5162100G-P|p=SAOS 100G SOFTWARE LICENSE, PERPETUAL | | |
| | | Properties: | | | | |
| | | Count | | 3 | | |
| | | Notice | | {product.Notice} | | |
| | | Host-id | | floating | | |
| | | State | | valid | | |
| | | Acquired-count | | 1 | | |
| | | Expiration: | | | | |
| | | Expiration-date | | 16-Nov-2018 | | |
| | | Last-renewal-date | | Fri Nov 9 06:09:38 2018 | | |
| | | Time-remaining | | 6 days, 23 hours, 49 mins, 5 secs | | |
| | | Type | | subscription | | |
| | | Issuer: | | | | |
| | | Issuer-name | | Ciena | | |
| | | Registration-id | | f6f3fd3233c3198e2d2af8acb60f46cbf0e743ea | | |
| | | Oper-state | | enabled | | |
| + |  | + | + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### License Server – primary and backup

***Objective:***

Verify primary and backup license servers can be provisioned.

***Procedure:***

* Go to the configuration terminal
  + config
* Enter the following command to create primary server
  + license-management-config license-server-config x.x.x.x eg:

license-management-config license-server-config 10.182.34.96

* Next, enter the following command to create backup server
* license-management-config license-server-config y.y.y.y backup **true**

primary-server x.x.x.x

Eg:

license-management-config license-server-config 10.182.34.96

license-management-config license-server-config 10.33.80.36 backup **true**

primary-server 10.182.34.96

* Display the license servers:

5170-0038-Node1> show license

+------- LICENSE SERVER STATE +

| Name | Value |

+ + +

| Primary Server | |

Hostname | 10.182.34.96

| |

| Server Port | 7071 |

| Oper State | enabled |

| Backup Server | |

Hostname | 10.33.80.36

| |

| Server Port | 7071 |

| Oper State | disabled |

| Refresh Period (h) | 12 |

+ + +

+ LICENSE CLIENT STATE +

| Name | Value |

+ + +

| Registration ID | a901cfdab0602893a71aea27b6822fd7a3314b6b |

| Oper State | enabled |

+ + +

+ LICENSE FEATURES BRIEF +

| | | Total | Acquired | Pending | Expiration |

| Feature Name | State | Count | Count | Count | Date |

+ + + + + + +

| SAOS-Adv\_100G\_5170 | valid | 1 | 1 | 0 | 12-May-2022 |

| SAOS-BaseOS\_AdvEth\_OAM\_5170 | valid | 1 | 1 | 0 | 12-May-2022 |

| SAOS-MPLS\_5170 | valid | 1 | 1 | 0 | 12-May-2022 |

| SAOS-Security\_5170 | valid | 1 | 1 | 0 | 12-May-2022 |

| SAOS-Sync\_5170 | valid | 1 | 1 | 0 | 12-May-2022 |

+ + + + + + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

#### Initial Access and Basic Configuration

###### Verify SAOS 10.x software version

***Objective:***

Objective is to verify Ciena SAOS 10.x installed.

***Procedure:***

* Login to CLI using the management IP you checked in the previous step:

ssh [diag@x.x.x.x](mailto:diag@x.x.x.x)

username: diag password: ciena123

* Issue the following command to verify
  + show software
* You should see an output like the following:

+ SOFTWARE STATE +

| Name | Value |

+ + +

| Current operation | idle |

| RPC Status | idle |

| Running package version | saos-10-01-00-0149 |

| Active bootchain | 01-01-00-0149 |

| Standby bootchain | 01-01-00-0149 |

+ + +

| Components: | |

| cn\_telemetry\_1 | 01-01-00-0149 |

| cn\_dhcp-ctrl\_1 | 01-01-00-0149 |

| cn\_alarm\_1 | 01-01-00-0149 |

| cn\_lacp\_1 | 01-01-00-0149 |

| cn\_collectd\_1 | 08-00-00-0165 |

| cn\_cnfp\_1 | 01-01-00-0149 |

| cn\_eoam\_1 | 01-01-00-0149 |

| cn\_dataplane\_1 | 01-01-00-0149 |

| cn\_feds\_1 | 01-01-00-0149 |

| cn\_dhcpl3relay\_1 | 01-01-00-0149 |

| cn\_snmp-agent\_1 | 01-01-00-0149 |

| cn\_svcdirectory\_1 | 01-01-00-0149 |

| cn\_cfm\_1 | 01-01-00-0149 |

| cn\_sync\_1 | 01-01-00-0149 |

| cn\_hal-dnx\_1 | 01-01-00-0149 |

| cn\_storage\_1 | 01-01-00-0149 |

| cn\_ui\_1 | 01-01-00-0149 |

| xg\_xgrade-agent\_1 | 08-00-00-0165 |

| cn\_central-logger\_1 | 08-00-00-0165 |

| cn\_sync-hal\_1 | 01-01-00-0149 |

| cn\_lldp\_1 | 01-01-00-0149 |

| cn\_ntp\_1 | 01-01-00-0149 |

| cn\_system\_1 | 01-01-00-0149 |

| cn\_ztp\_1 | 01-01-00-0149 |

| cn\_sat\_1 | 01-01-00-0149 |

| cn\_dns\_1 | 01-01-00-0149 |

| cn\_ipservices\_1 | 01-01-00-0149 |

| cn\_pkix\_1 | 01-01-00-0149 |

+ + +

| Available packages: | |

| saos-10-01-00-0149 | **activated** |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v2c Trap on the SAOS cli.

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY type trap tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v2c Inform Configuration

***SNMP v2c Inform:***

* + - * Informs are same as Traps but the main difference is that the Informs are acknowledged back by the SNMP Manager.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp community t1 security-name cienaSecurityV2c text-name cienaV2cCommunity snmp vacm view cienaAll include internet

snmp vacm group cienaGroup access "" v2c no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaGroup member cienaSecurityV2c security-model v2c snmp target TestTarget1 target-params TestParamsV2c udp ip 10.176.137.38 snmp target-params TestParamsV2c v2c security-name cienaSecurityV2c snmp target TestTarget1 tag TestTag

snmp notify Test-NOTIFY1 type inform tag TestTag

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY1 | TestTag | inform |

+ + + +

+ SNMP COMMUNITY +

| Community Index | Community Name | Security Name | Transport Tag |

+ + + + +

| t1 | cienaV2cCommunity | cienaSecurityV2c | |

+ + + + +

+ SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestParamsV2c | cienaSecurityV2c | | v2c | no-auth-no-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget1 | 10.176.137.38 | TestParamsV2c | TestTag | 162 | 3 | 1500 | 32 |

+ + + + + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+------------ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaGroup | v2c | cienaSecurityV2c |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaGroup | | exact | v2c | no-auth-no-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Get Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Get on the SAOS cli.

***SNMPv3 Get:***

* + - * User-based Security Model (USM) for Authentication and Encryption services.
      * First, we define the local users with different privilege levels.
      * The keys used in this example are regular strings converted into a HEX format.

o MD5 Key - cienaAuthKey - 63:69:65:6e:61:41:75:74:68:4b:65:79

o DES Key – cienaPrivKey - 63:69:65:6e:61:50:72:69:76:4b:65:79

* + - * Next, we define the Read Access and MIB View privileges for each user.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79 snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact read-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact read-view cienaAll snmp vacm group cienaV3Group access "" usm auth-priv context-match exact read-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp vacm view cienaAll include internet

***Output:***

* show snmp

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + + + + +

+ SNMP VACM VIEW +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + + +

+ SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | cienaAll | |

| cienaV3Group | | exact | usm | auth-no-priv | cienaAll | |

| cienaV3Group | | exact | usm | auth-priv | cienaAll | |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Trap Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Trap on the SAOS cli.

***SNMPv3 Trap:***

* + - * Same as the SNMP GET parameters but additional fields are added to specify the Trap target IP.

***Procedure:***

snmp usm local user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm local user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79 snmp usm local user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type trap

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | trap |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | local | | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthNoPrivUser | local | md5 | | 80:00:05:23:01:0A:78:67:F8:00:00 |

| cienaAuthPrivUser | local | md5 | des | 80:00:05:23:01:0A:78:67:F8:00:00 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### SNMP v3 Inform Configuration

***Objective:***

The objective of this section is to configure SNMP v3 Inform on the SAOS cli.

***SNMPv3 Inform:***

* + - * In the case of SNMPv3 when the agent sends an Inform Request to a manager it expects a

“reply” or acknowledgement from the manager. So, the manager is the authoritative entity.

* + - * Hence the users are defined as remote users and the snmpEngineID of the manager should be configured along with the username on the agent.
      * SNMP Inform are enabled by specifying the type as ‘inform’ whereas type ‘trap’ will be used

for SNMP traps.

***Procedure:***

snmp usm remote 80:00:05:23:01:0A:78:67:F8 user cienaNoAuthNoPrivUser exit

exit exit exit

snmp usm remote 80:00:05:23:01:0A:78:67:F8 user cienaAuthNoPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79

snmp usm remote 80:00:05:23:01:0A:78:67:F8 user cienaAuthPrivUser auth md5 key 63:69:65:6e:61:41:75:74:68:4b:65:79

snmp usm remote 80:00:05:23:01:0A:78:67:F8 user cienaAuthPrivUser priv des key 63:69:65:6e:61:50:72:69:76:4b:65:79

snmp vacm group cienaV3Group access "" usm no-auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-no-priv context-match exact notify-view cienaAll

snmp vacm group cienaV3Group access "" usm auth-priv context-match exact notify-view cienaAll snmp vacm group cienaV3Group member cienaNoAuthNoPrivUser security-model usm

snmp vacm group cienaV3Group member cienaAuthNoPrivUser security-model usm snmp vacm group cienaV3Group member cienaAuthPrivUser security-model usm snmp target TestTarget2 target-params TestUsmNoAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget2 tag TestTag

snmp target TestTarget3 target-params TestUsmAuthNoPriv udp ip 10.176.137.38 snmp target TestTarget3 tag TestTag

snmp target TestTarget4 target-params TestUsmAuthPriv udp ip 10.176.137.38 snmp target TestTarget4 tag TestTag

snmp target-params TestUsmNoAuthNoPriv usm security-level no-auth-no-priv user-name cienaNoAuthNoPrivUser

snmp target-params TestUsmAuthNoPriv usm security-level auth-no-priv user-name cienaAuthNoPrivUser

snmp target-params TestUsmAuthPriv usm security-level auth-priv user-name cienaAuthPrivUser snmp vacm view cienaAll include internet

snmp notify Test-NOTIFY tag TestTag type inform

***Output:***

* show snmp

+

SNMP NOTIFY +

| Notification Name | Notification Tag | Notification Type |

+ + + +

| Test-NOTIFY | TestTag | inform |

+ + +

+

+

SNMP USM +

| User Name | Type | Auth Protocol | Priv Protocol | Engine ID |

+ + + + + +

| cienaNoAuthNoPrivUser | remote | | | 80:00:05:23:01:0a:78:67:f8 |

| cienaAuthNoPrivUser | remote | md5 | | 80:00:05:23:01:0a:78:67:f8 |

| cienaAuthPrivUser | remote | md5 | des | 80:00:05:23:01:0a:78:67:f8 |

+ + +

+

+ + +

SNMP TARGET-PARAMS +

| Target Param Name | Security Name | User Name | Security Model | Security Level |

+ + + + + +

| TestUsmNoAuthNoPriv | | cienaNoAuthNoPrivUser | usm | no-auth-no-priv |

| TestUsmAuthNoPriv | | cienaAuthNoPrivUser | usm | auth-no-priv |

| TestUsmAuthPriv | | cienaAuthPrivUser | usm | auth-priv |

+ + +

+

+ + +

SNMP TARGET +

| Target Name | IP Address | Param Name | Tags | UDP Port | Retry Count | Timeout | Prefix Length |

+ + + + + + + + +

| TestTarget2 | 10.176.137.38 | TestUsmNoAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget3 | 10.176.137.38 | TestUsmAuthNoPriv | TestTag | 162 | 3 | 1500 | 32 |

| TestTarget4 | 10.176.137.38 | TestUsmAuthPriv | TestTag | 162 | 3 | 1500 | 32 |

+ + +

+ SNMP VACM VIEW +

+ + + + + +

| Viewtree Name | Subtree | Type |

+ + + +

| cienaAll | internet | include |

+ + + +

+ SNMP VACM GROUP MEMBER +

| Group Name | Security Model | Security Name |

+ + + +

| cienaV3Group | usm | cienaNoAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthNoPrivUser |

| cienaV3Group | usm | cienaAuthPrivUser |

+ + +

+

+

SNMP VACM GROUP ACCESS +

| Group Name | Context | Context Match | Security Model | Security Level | Read View | Notify View |

+ + + + + + + +

| cienaV3Group | | exact | usm | no-auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-no-priv | | cienaAll |

| cienaV3Group | | exact | usm | auth-priv | | cienaAll |

+ + + + + + + +

***Test Case Results:***

Passed: Yes No Verified by Date/Time Comments

###### Syslog Setup

***Objective:***

Objective is to validate syslog server setup. This test is a continuation of the Source IP testcase.

***Procedure:***

* Enter the management IP on 10x node. The node in this testcase is in-band managed via a routable loopback interface “lb1”.
  + show ip interfaces brief

3928-003> show ip int b

+ IP INTERFACES BRIEF +

| | | | | Status | | Underlay |

| Interface | IP Address | VRF | Origin | Admin | Oper | Role | Binding |

+ + + + + + + + +

| mgmtbr0 | 10.181.35.227 | default | STATIC | DOWN | DOWN | management | - |

| remote | unassigned | default | - | UP | UP | management | remote-fd |

**| lb1 | 10.181.102.165 | default | STATIC | UP | UP | management | -** |

| if10 | 172.18.1.2 | default | STATIC | UP | UP | data | VLAN4001 |

| if9 | 172.18.2.1 | default | STATIC | UP | UP | data | VLAN4002 |

+ + + + + + + + +

* Setup the syslog server
  + syslog log-actions remote dest 10.181.65.17 admin-state enabled
* Validate the syslog setup on the node.

3928-003> show syslog

+--- REMOTE --+

| Admin-State |

+ +

| enabled |

+ +

+ DESTINATION +

| Server IP | Admin-State | Port | Facility | Severity | Custom prefix |

+ + + + + + +

| 10.181.65.17 | enabled | 514 | ietf-syslog-types:local6 | info | |

+ + + + + + +

* Show management plane default, currently the node does not have the default source IP set to the loopback “lb1”.

3928-003> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| |

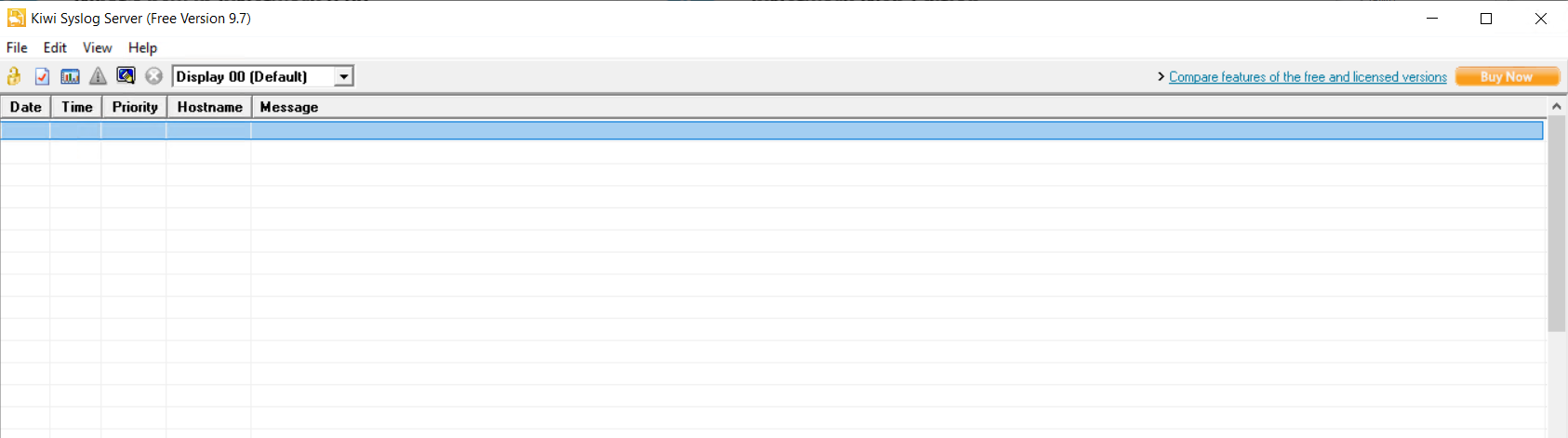
+ +

* Disable a logical port and check on syslog server for any messages received on the syslog server.

diag@3928-003# logical-ports logical-port 10 admin-state disable Applying 1 edit

diag@3928-003# logical-ports logical-port 10 admin-state enable Applying 1 edit

* There are no messages received on syslog server.



* Set the management source ip on the node as the “lb1”.

management-plane default-source-ip interface lb1

* Show the management-plane source IP on node

3928-003> show management-plane

+ DEFAULT SOURCE IP INTERFACE +

| Interface |

+ +

| lb1 |

+ +

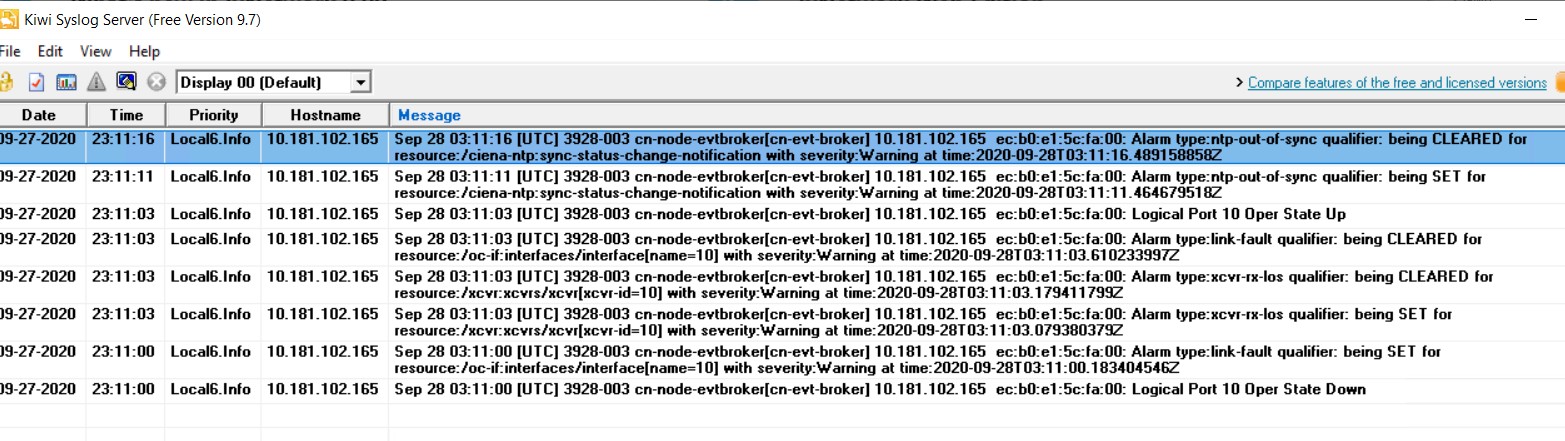
* Disable a logical port and check on syslog server for any messages received on the syslog server.

diag@3928-003# logical-ports logical-port 10 admin-state disable

Applying 1 edit diag@3928-003#

diag@3928-003# logical-ports logical-port 10 admin-state enable Applying 1 edit

* Validate on the syslog server that the messages have been received. Messages have been received on the syslog server.



* To delete the syslog server:

no syslog

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### TLS profiles

***Objective:***

Objective is to setup TLS profiles for use in Telemetry and SZTP.

***Procedure:***

* Enter the following command on CLI to create a TLS Service Profile:

config

*pkix peer-auth-profiles peer-auth-profile peer-auth- profile check-cert-expiry true*

*hello-params tls-profile cipher-suites cipher-suite ecdhe-rsa-with-aes-128-cbc-sha*

*hello-params tls-profile elliptic-curves elliptic- curve ciena-tls-types:secp256r1*

*hello-params tls-profile session-resumption-timeout 600*

*tls-service-profiles test tls-profile-name tls- profile*

*tls-service-profiles test tls-peer-auth-profile-name peer-auth-profile*

*tls-service-profiles test tls-certificate-name testCert*

* Then attach Telemetry and SZTP to the test TLS profile:

telemetry-system server config tls-service-profile test ztp tls-service-profile test

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Pkix and TLS- IP host list

***Objective:***

Secure TLS require PKIX ( public key infrastructure / X.509) to manage the devices private keys and CA and device certificates. New enhancement introduced in SAOS 10.4 and onwards – check IP host list (while peer authentication). Check IP host allows the user to specify which devices are allowed to connect to it. The user configures a list of acceptable IP addresses and DNSs then enables check IP host. The list is cross-referenced with either the Subject Alternate Name or the Common Name of the certificate. If it matches, then a TLS connection will be allowed.

***Procedure:***

* Add entries to ip-host-list:

pkix peer-auth-profiles peer-auth-profile <peer-auth- profile-name> ip-host-list <ip-address|hostname> <ip- address|hostname> <ip-address|hostname>

* Enable check IP/host:

pkix peer-auth-profiles peer-auth-profile <peer-auth- profile-name> check-ip-host true

* Validate with below commands

5170-208> show tls

+ TLS SERVICE PROFILES +

| Name | Value |

+ + +

| Service Profile Name | test |

| TLS Profile Name | tls-profile |

**|** Peer Auth Profile Name | https-peer-auth-profile |

| Certificate Name | testCert |

+ + +

+----------- **PEER AUTH PROFILES** +

| Name | Value |

+ + +

| Profile Name | https-peer-auth-profile |

| Check Expiry | True |

| Check IP/Host | True |

| IP/Host List | 10.121.190.169 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Telemetry

***Objective:***

Objective is to verify Telemetry with PKIX certificates. This testcase is related to the PKIX testcase.

***Procedure:***

* Setup a gnmi-client on a linux server. For this test, the gnmi-client is setup on the server/VM 10.181.65.91.
* Download the certificates from CA server to the node.

pkix-certificates install login-id ftpuser password ciena123 cert-name cert-openssl-1.1.1 cert-passphrase ciena remote-file-uri <ftp://10.181.65.91/~/gnmi/ValimarDevServer-openssl-1.1.1.p12> cert-only false

pkix-ca install login-id ftpuser password ciena123 ca-cert-name ValimarCa remote-file-uri [ftp://10.181.65.91/~/gnmi/ValimarDevCa-](ftp://10.181.65.91/~/gnmi/ValimarDevCa-openssl-1.1.1.cert.pem) [openssl-1.1.1.cert.pem](ftp://10.181.65.91/~/gnmi/ValimarDevCa-openssl-1.1.1.cert.pem)

* Validate that the certificates have been downloaded:

3928-003> show pkix

+ CA CERTIFICATES +

| Name | Value |

+ + +

| CA Name | ValimarCa |

| Subject Common Name | |

| Issuer Common Name | |

| Valid Until | Aug 8 23:19:19 2040 UTC (19 years) |

+ + +

+---- CERTIFICATE REVOCATION LISTS ---+

| Name | Value |

+ + +

| No Entries |

+ + +

+ DEVICE CERTIFICATES +

| Name | Value |

+ + +

| Certificate Name | cert-openssl-1.1.1 |

| Algorithm ID | - |

| Private Key | present |

| Subject Common Name | ValimarDevServer-openssl-1.1.1-rsa4096 |

| Issuer Common Name | - |

| Valid Until | Aug 24 21:40:12 2021 UTC (10 months) |

+ + +

* Setup TLS, PKIX, and Telemetry server.

hello-params tls-profile cipher-suites cipher-suite ecdhe-rsa- with-aes-128-cbc-sha

hello-params tls-profile elliptic-curves elliptic-curve ciena- tls-types:secp256r1

hello-params tls-profile session-resumption-timeout 3600 pkix peer-auth-profiles peer-auth-profile peer-auth-profile check-cert-expiry true

tls-service-profiles test tls-profile-name tls-profile

tls-service-profiles test tls-peer-auth-profile-name peer-auth- profile

tls-service-profiles test tls-certificate-name cert-openssl- 1.1.1

telemetry-system server config enable true

telemetry-system server config tls-service-profile test exit

* Validate TLS setup:

3928-003> show tls

+------------ TLS SERVICE PROFILES +

| Name | Value |

+ + +

| Service Profile Name | test |

| TLS Profile Name | tls-profile |

| Peer Auth Profile Name | peer-auth-profile |

| Certificate Name | cert-openssl-1.1.1 |

+ + +

+---------- PEER AUTH PROFILES +

| Name | Value |

+ + +

| Profile Name | peer-auth-profile |

| Check Expiry | True |

| Check IP/Host | - |

| Check Fingerprint | - |

| Fingerprint List | - |

+ + +

+ HELLO PARAMS +

| Name | Value |

+ + +

| Profile Name | tls-profile |

| Protocol Versions | tls-1.2 |

| Cipher Suites | ecdhe-rsa-with-aes-128-cbc-sha |

| Elliptic Curves | secp256r1 |

| Sess. Resumption Timeout (s) | 3600 |

| OCSP State | disabled |

| NONCE State | enabled |

| Default OCSP Responder URL | - |

+ + +

* Subscribe to a sensor from the gnmi-client and validate that messages are being received. Output from GNMI-client on remote server polling for 10x node system memory:

ftpuser@ftpuser:~/gnmi$

gnmi\_cli -a 10.181.102.165:6702 -updates\_only -qt s -dt s - sample\_interval 50000 -client\_types gnmi -insecure -client\_crt Vali marDevClient-openssl-1.1.1.cert.pem -client\_key ValimarDevClient- openssl-1.1.1.key.pem -with\_user\_pass -q **/ciena-sys-tmet:system- state/memory**

username: diag password:

Ciena/ciena-sys-tmet:system-state/memory/active, 2189152256

Ciena/ciena-sys-tmet:system-state/memory/available, 1533530112

Ciena/ciena-sys-tmet:system-state/memory/buffers, 684834816

Ciena/ciena-sys-tmet:system-state/memory/cached, 895356928

Ciena/ciena-sys-tmet:system-state/memory/free, 213032960

Ciena/ciena-sys-tmet:system-state/memory/inactive, 697450496

Ciena/ciena-sys-tmet:system-state/memory/total, 4113903616

Ciena/ciena-sys-tmet:system-state/memory/used, 2320678912

Ciena/ciena-sys-tmet:system-state/memory/used-percent, 62.7

Ciena/ciena-sys-tmet:system-state/memory/active, 2189561856

Ciena/ciena-sys-tmet:system-state/memory/available, 1534181376

Ciena/ciena-sys-tmet:system-state/memory/buffers, 684843008

Ciena/ciena-sys-tmet:system-state/memory/cached, 895713280

Ciena/ciena-sys-tmet:system-state/memory/free, 213442560

* Verify telemetry sensor subscription:

3928-003> show telemetry subscriptions

+--------------------------- TELEMETRY SUBSCRIPTIONS +

| Index | Name | Value |

+ + + +

| 1 | Subscription: | |

| | Subscription-ID | 4ca324bf-db60-48ea-9e3b-6325346268e0 |

| | Subscription State | |

| | User Name | diag |

| | Subscription Mode | stream |

| | Update Only | True |

| | Sample Interval | 5000000000 |

| | Subscription Message | |

| | Telemetry Sensor Paths | |

| | Telemetry Sensor Path | /ciena-sys-tmet:system-state/memory |

| | Telemetry Sensor ID | 17435055178426406752 |

| | Telemetry Sensor Sub-Mode | target-defined |

+ + + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### RADIUS over TLS configuration

***Objective:***

Objective is to successfully authenticate to a Ciena device using RADSEC.

***Procedure:***

* Download the CA and Device Certificates:

pkix-ca install ca-cert-name RADSECCA remote-file-uri sftp://1.1.1.1/home/tls/certs/RadSecClntCA.pem login-id tls password tls pkix-certificates install cert-name RADSECCLIENT cert-only **false** remote- file-uri sftp://1.1.1.1/home/tls/certs/RadSecClntCert.p12 cert- passphrase ciena123 login-id tls password tls

* Then create TLS Profile configuration (can also follow TLS profile step in the document):

hello-params TLS\_PROFILE1 cipher-suites cipher-suite rsa-with-aes-256- cbc-sha

hello-params TLS\_PROFILE1 elliptic-curves elliptic-curve ciena-tls- types:secp256r1

hello-params TLS\_PROFILE1 session-resumption-timeout 3600 hello-params TLS\_PROFILE1 tls-versions tls-version tls-1.2

pkix peer-auth-profiles peer-auth-profile PAPROFILE1 check-cert- expiry **true**

tls-service-profiles TLS\_SRVR\_PROFILE1 tls-profile-name TLS\_PROFILE1 tls-service-profiles TLS\_SRVR\_PROFILE1 tls-peer-auth-profile-name PAPROFILE1

tls-service-profiles TLS\_SRVR\_PROFILE1 tls-certificate-name RADSECCLIENT

* Then Create AAA configuration:

system aaa accounting config accounting-method RADSERVER

system aaa accounting events event AAA\_ACCOUNTING\_EVENT\_LOGIN config event-type AAA\_ACCOUNTING\_EVENT\_LOGIN

system aaa accounting events event AAA\_ACCOUNTING\_EVENT\_LOGIN config record START\_STOP

system aaa server-groups server-group RADSERVER config name RADSERVER system aaa server-groups server-group RADSERVER config type RADSEC system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 config address 1.1.1.1

system aaa server-groups server-group RADSERVER servers server 1.1.1.1 config admin-state enabled

system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 radsec config tls-service-profile TLS\_SRVR\_PROFILE1 system aaa server-groups server-group RADSERVER servers

server 1.1.1.1 config name radsecserver

* Last step is to configure Authentication parameters:

system aaa authentication config authentication-method RADSERVER no system aaa authentication config authentication-method AUTH\_LOC system aaa authentication config authentication-method AUTH\_LOC

NOTE: for server configuration you can refer to the following confluence page. <https://confluence.ciena.com/pages/viewpage.action?pageId=603288778>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Syslog over TLS configuration

***Objective:***

Objective is to successfully generate Syslog messages over a secure TLS session.

***Procedure:***

* Download the CA and Device Certificates:

pkix-ca install ca-cert-name SYSLOGCA remote-file-uri sftp://1.1.1.1/home/tls/certs/SyslogCA.pem login-id tls password tls pkix-certificates install cert-name SYSLOGCLIENT cert-only **false** remote- file-uri sftp://1.1.1.1/home/tls/certs/SyslogClntCert.p12 cert- passphrase ciena123 login-id tls password tls

* Then create TLS Profile configuration (can also follow TLS profile step in the document):

hello-params 'TLS\_PROFILE2' tls-versions tls-version tlscmn:tls-1.2 hello-params 'TLS\_PROFILE2' cipher-suites cipher-suite tlscmn:rsa-with- aes-256-cbc-sha

hello-params 'TLS\_PROFILE2' elliptic-curves elliptic-curve ciena-tls- types:secp256r1

tls-service-profiles TLS\_SRVR\_PROFILE2 tls-profile-name TLS\_PROFILE1 tls-service-profiles TLS\_SRVR\_PROFILE2 tls-peer-auth-profile-name PAPROFILE1

tls-service-profiles TLS\_SRVR\_PROFILE2 tls-certificate-name SYSLOGCLIENT

* Then configure Syslog:

syslog log-actions remote-syslog-tls admin-state disabled tls-service- profile "TLS\_SRVR\_PROFILE2"

syslog log-actions remote-syslog-tls destination '1.1.1.1' severity alert critical debug emergency error info notice warning

* The last step is to verify that the transport error = Success:

CN5166-0004-R203> show syslog tls statis

+--------- SYSLOG TLS SERVER STATISTICS +

| Name | Value |

+ + +

| Server Address | 1.1.1.1 |

| Oper State | enabled |

| Connection Attempts | 1 |

| Successful Connections | 1 |

| Failed-tcp Connections | 0 |

| Failed-tls Connections | 0 |

| timed-out-connections | 0 |

| Unexpected Close Connections | 0 |

| Closed Connections | 0 |

| Last Transport Error | Success |

+ + +

NOTE: for server configuration you can refer to the following confluence page. <https://confluence.ciena.com/pages/viewpage.action?pageId=614967766>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SSH Public Key Authentication

***Objective:***

Authenticate to the device with a public key instead of a password.

***Procedure:***

* Generate the public private key pair on the client (note that this will depend on the client in use. Example below is a Linux client):

*ssh-keygen -t rsa -b 2048 -N "" -f key\_pair*

* Install the Public key on the device:

ssh-user-pubkey-install user diag url <http://1.1.1.1/pub.key>

* Configure SSH server (example below):

system ssh-server config encryption-algorithm aes256-cbc system ssh-server config mac-algorithm hmac-sha2-256

system ssh-server config kex-algorithm diffie-hellman-group14-sha256 system ssh-server config pka-algorithm ssh-rsa

* Enable public key authentication:

system ssh-server config public-key-authentication enabled

* Verify public key is installed and associated with correct user:

CN5166-0004-R203> show system ssh-server user-pubkey user-name diag

+ SSH USER PUBLIC KEYS +

| Name | Value |

+ + +

| User | diag |

| Fingerprint(MD5) | 56:15:0a:04:15:0c:09:b8:60:f5:1f:c4:f2:44:09:72 |

| Fingerprint(SHA-1) | cJYRbUOM0C3MmF3FhMbVRhgn2AU |

+ + +

* Verify Encryption algorithm is correct :

CN5166-0004-R203> show system ssh-server config

+ SSH SERVER CONFIG +

| Name | Value |

+ + +

| Encryption Algorithm | aes256-cbc |

| Kex Algorithm | diffie-hellman-group14-sha256 |

| MAC Algorithm | hmac-sha2-256 |

| Public Key Algorithm | ssh-rsa |

| Public Key Authentication | enabled |

| Rekey Limit | 500M |

| Rekey Time | None |

+ + +

* Authenticate to the device with client and key

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### SSH Rekeying Configuration

***Objective:***

Configure SSH rekeying and verify configuration.

***Procedure:***

* Configure SSH max time in seconds after which SSH key is renegotiated:

system ssh-server config rekey-time 300

* Configure SSH max data exchanged before SSH key is renegotiated:

system ssh-server config rekey-limit 1G

* Verify rekey configuration is applied:

CN5166-0004-R203> show system ssh-server config

+ SSH SERVER CONFIG +

| Name | Value |

+ + +

| Encryption Algorithm | aes256-cbc |

| Kex Algorithm | diffie-hellman-group14-sha256 |

| MAC Algorithm | hmac-sha2-256 |

| Public Key Algorithm | ssh-rsa |

| Public Key Authentication | enabled |

| Rekey Limit | 1G |

| Rekey Time | 300seconds |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DNS Client Setup

***Objective:***

Objective is to verify setting up DNS client

***Procedure:***

* Enter the following command on CLI with an example DNS server 192.168.10.100:

config

*oc-sys:system dns dns-client admin-status enabled*

*oc-sys:system dns dns-client domain-name ott.ciena.com oc-sys:system dns dns-client server 192.168.10.100*

* You should see something like the following:

5170-010> show dns

+ DNS-CLIENT +

| Name | Value |

+ + +

| Admin-status | enabled |

| Domain-name | ott.ciena.com |

| Domain-name-scope | user |

| Server-scope | user |

+ + +

+ USER-SERVERS +

| IP Address | Oper-status |

+ + +

| 192.168.10.100 | enabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### L3 DHCPv4 Relay Setup

***Objective:***

Objective is to setup L3 DHCP Relay (IPv4 only).

VLAN 51 VLAN 52



192.168.2.15/24

192.168.2.14/24

192.168.1.16/24

51xx,3 5170

DHCP L3 DHCP Server

192.168.1.101

***Procedure:***

* Create the classifier and flow points and forwarding domains on the L3 DHCP Relay :

***#Classifiers***

config

classifiers classifier vlan51 filter-entry vtag-stack vtags 1 vlan-id 51

classifiers classifier vlan52 filter-entry vtag-stack vtags 1 vlan-id 52

exit

***#Forwarding-domains***

config

fds fd FDRelayClient mode vpls fds fd FDRelayServer mode vpls

exit

***#Flow-points***

config fps

fp fp15

fd-name FDRelayClient logical-port 15

classifier-list-precedence 7 stats-collection on classifier-list vlan51

mtu-size 2000

egress-l2-transform push-vid-51 vlan-stack 1

push-tpid tpid-8100 push-vid 51

exit exit exit exit

fps

fp fp16

fd-name FDRelayServer logical-port 16

classifier-list-precedence 7 stats-collection on classifier-list vlan52

mtu-size 2000

egress-l2-transform push-vid-52 vlan-stack 1

push-tpid tpid-8100 push-vid 52

exit exit exit

***#IP interfaces***

oc-if:interfaces interface if15 config name if15 vrfName default cn- if:type ip mtu 2000 admin-status true underlay-binding config fd FDRelayClient

oc-if:interfaces interface if15 ipv4 addresses address 192.168.2.15 config ip 192.168.2.15 prefix-length 24

oc-if:interfaces interface if16 config name if16 vrfName default cn- if:type ip mtu 1500 admin-status true underlay-binding config fd FDRelayServer

oc-if:interfaces interface if16 ipv4 addresses address 192.168.1.16 config ip 192.168.1.16 prefix-length 24

* Configure L3 Relay:

config

l3-relay-agent instance toi\_dtw admin-enabled true

dhcp-server-addresses 192.168.1.101

ip-interfaces if15

flow-points fp15 flow-point-trusted true

cid-string cid-client

ip-interface-enabled true ip-interface-trusted true exit

ip-interfaces if16

flow-points fp16 flow-point-trusted true cid-string cid-server

ip-interface-enabled true ip-interface-trusted true

* Display L3 Relay Configuration:

5170-010> show dhcpl3relay

+---- DHCP L3 RELAY CONFIGURATION +

| Name | Value |

+ + +

| Instance | toi\_dtw |

| Admin State | Enabled |

| Circuit ID Type | String |

| Remote ID Type | String |

| Remote ID String | rid-server |

| Option 82 | On |

| DHCP Server(s) | 192.168.1.101 |

| IP Interface | if15 |

| Circuit ID String | cid-client |

| Admin State | Enabled |

| Trust State | Trusted |

| IP Interface | if16 |

| Circuit ID String | cid-server |

| Admin State | Enabled |

| Trust State | Trusted |

+ + +

+ DHCP L3 RELAY STATUS +

| Name | Value |

+ + +

| Instance | toi\_dtw |

| Status Message | Interface if15 is not configured with an IPv4 address |

| Operational State | Disabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### DHCPv6 Client Setup

***Objective:***

Ensure that with DHCPv6 client enabled, the interface will acquire an IPv6 address automatically. **Only stateful DHCPv6 (no SLAAC) is currently supported.**

***Procedure:***

* Dual IPv4 and IPv6 stack on mgmt. interfaces are supported as of 10.3 and onwards. Enable DHCPv6 client on mgmtbr0. Ensure that :
  + config
  + dhcpv6-client client mgmtbr0 admin-enable true
* Configure IPv4 static IP on the mgmtbr0 as well.
  + dhcp-client client mgmtbr0 admin-enable false
  + oc-if:interfaces interface mgmtbr0 ipv4 address address x.x.x.x config ip x.x.x.x prefix-length 20
  + rib vrf default ipv4 x.x.x.x/8 next-hop x.x.x.x description "lab default"

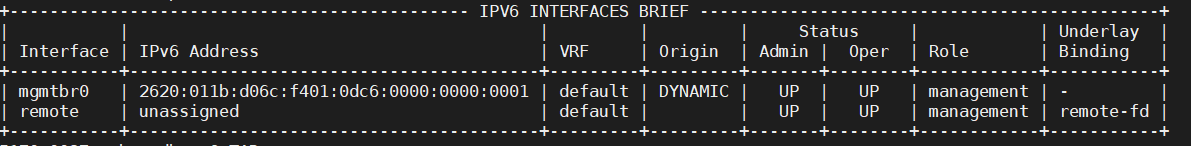
Ex:

dhcp-client client mgmtbr0 admin-enable false

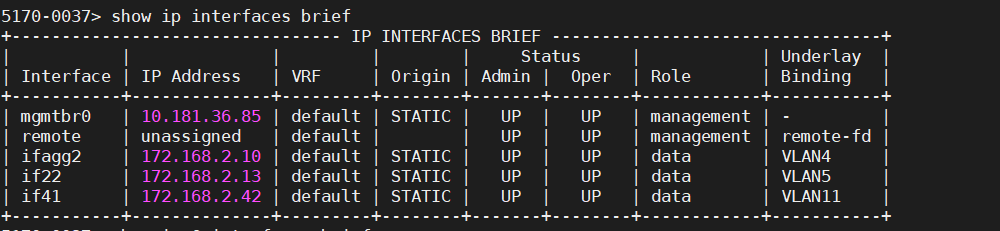
oc-if:interfaces interface mgmtbr0 ipv4 address address 10.181.36.85 config ip 10.181.36.85 prefix-length 20

rib vrf default ipv4 10.0.0.0/8 next-hop 10.181.32.1 description "lab default"

* Display the IPv6 and IPv4 interfaces on the node.
  + 5170-0037> show ipv6 interfaces brief



* + 5170-0037> show ip interfaces brief



5170-0037> show dhcpv6

+-------- DHCPV6 CLIENT CONFIGURATION +

| Name | Value |

+ + +

| Interface Name | mgmtbr0 |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

| Interface Name | remote |

| Admin State | Enabled |

| Rapid Commit | Enabled |

| Requested Preferred Lifetime (s) | 0 |

| Requested Valid Lifetime (s) | 0 |

| Option | |

| DNS Server List | Enabled |

| Domain Search List | Enabled |

| Posix Time Zone | Disabled |

| TZDB Time Zone | Enabled |

| NTP Server | Enabled |

| Bootfile URL | Enabled |

+ + +

+ DHCPV6 CLIENT STATE +

| Name | Value |

+ + +

| Interface Name | remote |

| Oper State | Enabled |

| DHCPv6 State | preinit |

| Config State | stateful |

| Renewal (T1) Time (s) | |

| Renewal (T1) Time Remaining (s) | |

| Rebinding (T2) Time (s) | |

| Rebinding (T2) Time Remaining (s) | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  | | Preferred Lifetime (s) Preferred Lifetime Remaining Valid Lifetime (s)  Valid Lifetime Remaining (s) | (s) | |  |  |  | |  | |  |  |  | |
| |  |  |  |  |  |  |  |  +  | | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL  Interface Name |  | |  |  |  |  |  |  |  |  +  | | mgmtbr0 | |  |  |  |  |  |  |  |  +  | |
| **|**  **|**  **|**  | | **Oper State DHCPv6 State Config State**  Renewal (T1) Time (s) |  | **|**  **|**  **|**  | | **Enabled bound stateful**  302400 | **|**  **|**  **|**  | |
| | | Renewal (T1) Time Remaining | (s) | | | 241733 | | |
| | | Rebinding (T2) Time (s) | | | | 453600 | | |
| | | Rebinding (T2) Time Remaining (s) | | | | 392933 | | |
| | | Preferred Lifetime (s) | | | | 604800 | | |
| | | Preferred Lifetime Remaining (s) | | | | 544133 | | |
| | | Valid Lifetime (s) | | | | 604800 | | |
| | | Valid Lifetime Remaining (s) | | | | 544133 | | |
| |  |  |  |  |  |  |  |  + | DHCPv6 Server DUID Option Value  DNS Server List Domain Search List Posix Time Zone TZDB Time Zone  NTP servers Boot File URL | | |  |  |  |  |  |  |  |  + | 0:1:0:1:25:22:d:24:0:0:5e:0:1:81 | |  |  |  |  |  |  |  |  + |

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Static Mgmt IPv6 Setup

***Objective:***

Static IPv6 address can be added onto management interface.

***Procedure:***

* Disabled DHCPv6 client. DHCVPv6 client is enabled by default.

config

* + dhcpv6-client client mgmtbr0 admin-enable false
* Then configure a static IPv6 address:

oc-if:interfaces interface mgmtbr0 ipv6 address address x.x.x.x.x.x.x.x config ip x.x.x.x.x.x.x prefix-length y

rib vrf default ipv6 x.x.x.x.x.x.x.x/y next-hop x.x.x.x.x.x.x.x description "lab default"

* Example :

## Disable DHCPv6 Client

dhcpv6-client client mgmtbr0 admin-enable false

## Setup IPv6 mgmtbr mgmt. interface

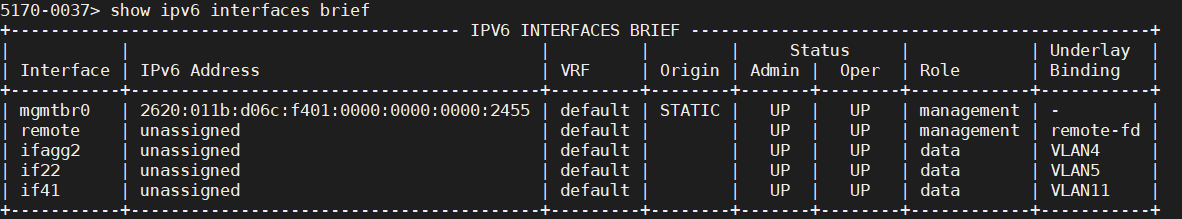
oc-if:interfaces interface mgmtbr0 ipv6 addresses address 2620:11b:d06c:f401::2455 config ip 2620:11b:d06c:f401::2455

prefix-length 64

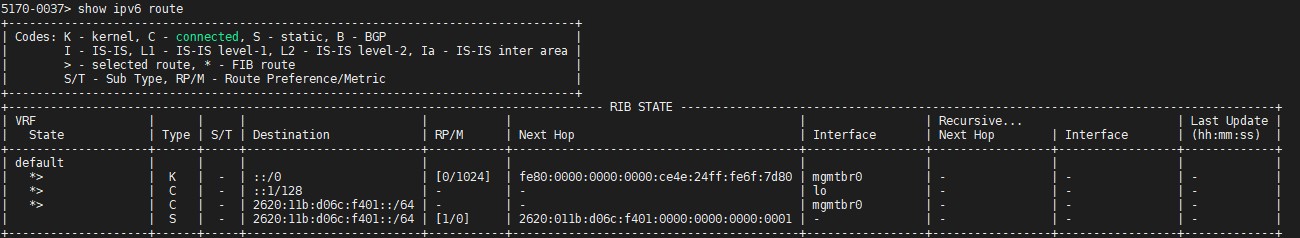
## Setup IPv6 static route to gateway router

rib vrf default ipv6 2620:011b:d06c:f401::2455/64 next-hop 2620:011b:d06c:f401::1

* Check the provisioning:
  + show ipv6 interfaces brief



* + show ipv6 route



Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configuration – Golden Configuration

***Objective:***

Objective is to verify backup and restore of the golden configuration. Golden configuration is a backup file which contains pre-staging configuration for xZTP. From CLI, the user can perform a reset to golden-config to put system back to perform xZTP. Hence, this enables the operator to have a failsafe configuration file.

***Procedure:***

* On Valimar cli, perform a backup to golden-config. Normally, the golden config should contain basic infrastructure provisioning such mgmt. interfaces, remote servers such as authentication servers/syslog/SNMP etc….
  + system backup golden-config
* Perform a system reset to factory-default by push button. This can take 15-20minutes to complete. After system is reset, user can login with default login of diag/ciena123 from the console port. The node should only have golden-config provisioning on the system.
* Alternatively, the user can execute a cli command to reset provisioning to golden-config.
  + 3928> system reset golden-config

PRESS <CTRL>C TO ABORT (10 seconds) PRESS <CTRL>C TO ABORT (9 seconds) PRESS <CTRL>C TO ABORT (8 seconds) PRESS <CTRL>C TO ABORT (7 seconds) PRESS <CTRL>C TO ABORT (6 seconds) PRESS <CTRL>C TO ABORT (5 seconds) PRESS <CTRL>C TO ABORT (4 seconds) PRESS <CTRL>C TO ABORT (3 seconds) PRESS <CTRL>C TO ABORT (2 seconds) PRESS <CTRL>C TO ABORT (1 seconds)

proceeding to reboot

* To delete the golden-config, enter the following command:
  + system delete golden-config

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Port Flap Detection

Port flapping results from instability in the network where the ports toggles up and down within a short span of time. The port flapping results in network to re-converge when the state of the port/link changes. Port Flap Detection feature will detect port flaps and apply a hold timer before changing the state of the port to down

***Objective:***

Enable port flap detection and set the necessary parameters.

***Procedure:***

* Enable port flap detection.
  + oc-if:interfaces interface <port-id> config link-flap- detect true
* Set the time window to detect the link flaps.
  + oc-if:interfaces interface <port-id> config link-flap- detect-time <detect-time value> (default = 10s)
* Set the number of link flaps that would occur during the time window that will trigger a port down.
  + oc-if:interfaces interface <port-id> config link-flap- count <flap-count value> (default = 5s)
* Set the amount of time the link should be held down when too many link flaps have been detected.
  + oc-if:interfaces interface <port-id> config link-flap- hold-time <hold-time value> (default = 300s)
* Verify the settings:

5162-001> show ettps ettp 42

+ Ettp +

| KEY | VALUE |

+ + +

| Name | 42 |

| Description | 42 |

| Type | ettp |

| Admin Status | True |

| Mode | auto |

| Link Flap Detect | True |

| Link Flap Count | 5 |

| Link Flap Detect Time | 10 |

| Link Flap Hold Time | 300 |

| Duplex | full |

| Port Speed | 100Gb |

| Flow Control | off |

| Auto Negotiation | False |

| Forward Error Correction | auto |

+ + +

* Verify the statistics:

5162-001> show ettps ettp 2 statis

+ Ettp +

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| | | KEY | | | VALUE | | |
| + |  | + |  | + |
| | | Name | | | 2 | | |
| | |  | | |  | | |
| | |  | In Bytes | | 0 | | |
| | |  | In Unicast Packets | | 0 | | |
| | |  | In Errors | | 0 | | |
| | |  | Out Unicast Pkts | | 0 | | |
| | |  | Out Errors | | 0 | | |
| | |  | In Pkts | | 0 | | |
| | |  | Out Bytes | | 15834974 | | |
| | |  | Out Pkts | | 138696 | | |

| Link Flap Events | 0 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Low Latency Bypass (currently only available on 5162)

***Objective:***

Enable low latency bypass. LLBP can only be enabled on 5162. This feature enable a specific internal datapath to support performance and scale for features such as IP BFD and CFM.

***Procedure:***

* Unbind the logical port 40.
  + no logical-ports logical-port 40 binding
* Activate interface 40’s LLBP.
  + oc-if:interfaces interface 40 config offload-activate true
* This will enable a lower latency internal data path.

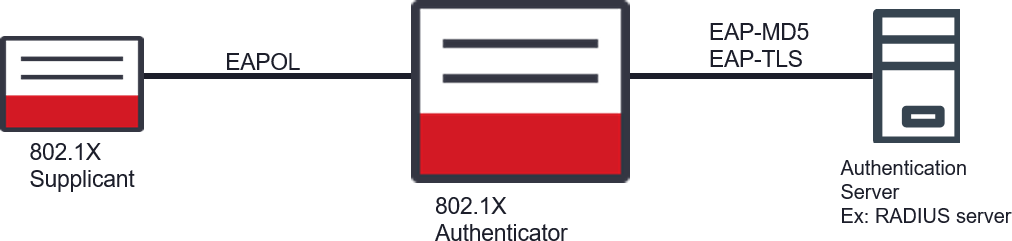
Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Dot1X – Supplicant Setup

***Objective:***

Verify the dot1x supplicant setup.



***Procedure:***

* Enable dot1x globally on system.
  + system dot1x config system-auth-control enabled
* Set the port to “supplicant”.
  + oc-if:interfaces interface 17 config dot1x port- capabilities supplicant true
  + oc-if:interfaces interface 17 config dot1x supplicant admin-status enabled
* Set the identity and password of the Supplicant.
  + oc-if:interfaces interface 17 config dot1x supplicant identity seitoi
  + oc-if:interfaces interface 17 config dot1x supplicant password seitoi
* Display Supplicant information.

5162-0027> show dot1x ports supp port 17

+ DOT1X PORT SUMMARY +

| Name | Value |

+ + +

| Port Name | 17 |

| Admin State | Enabled |

| Start Period (sec) | 30 |

| Held Period (sec) | 60 |

| Auth Period (sec) | 30 |

| Max Start | 3 |

| Username | **seitoi** |

| Password | Set |

| EAP Version | 2 |

| EAP Method | md5 |

| Operational State | **Enabled** |

| Controlled Port Status | Unauthorized |

| PAE State | Held |

| Last EAPOL Frame Version | 0 |

| Last EAPOL Frame Source | 00:00:00:00:00:00 |

+

+

--+

+ +

DOT1X PORT STATISTICS

| | Eapol | Eapol | Eapol Start | Eapol Logoff | Invalid Eapol | Eapol Length |

| Port | Frame Tx | Frame Rx | Frame Tx | Frame Tx | Frame Rx | Error Frames |

+ + + + + + +

--+

| 17 | 5 | 0 | 5 | 0 | 0 | 0

|

+ + + + + + +

--+

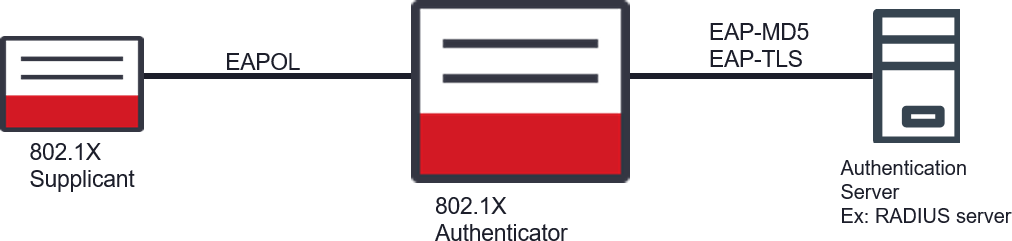
Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Dot1X – Authenticator Setup

***Objective:***

Verify the dot1x Authenticator setup.



***Procedure:***

* Enable dot1x globally on system.
  + system dot1x config system-auth-control enabled
* Set the port to “authenticator”.
  + oc-if:interfaces interface 17 config dot1x port- capabilities authenticator true
  + oc-if:interfaces interface 17 config dot1x authenticator admin-status enabled/disabled
* Display Authenticator information.

5162-0028> show dot1x ports auth port 17

+ DOT1X PORT SUMMARY +

| Name | Value |

+ + +

| Port Name | 17 |

| Admin State | Enabled |

| Port Control | Auto |

| ReAuth Enabled | False |

| Quiet Period (sec) | 60 |

| Server Timeout (sec) | 30 |

| ReAuth Period (sec) | 3,600 |

| Max Retries | 2 |

| EAP Version | 2 |

| Control Direction | Both |

| Operational State | Disabled |

| Controlled Port Status | Unauthorized |

| Last EAPOL Frame Version | 0 |

| Last EAPOL Frame Source | 00:00:00:00:00:00 |

+ + +

+

+

DOT1X PORT STATISTICS

| | Eapol | Eapol | Eapol Start | Eapol Logoff | Eapol Resp | Eapol Resp | Eapol Req | Invalid Eapol | Eapol Req | Eapol Length |

| Port | Frame Tx | Frame Rx | Frame Rx | Frame Rx | Id Rx | Rx | Tx | Frame Rx | Id Tx | Error Frames |

+ + + + + + + +

+ + + +

| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0

| 0 | 0 | 0 |

+ + + + +

+ + +

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Set up LLDP Global Config

***Objective:***

Objective is to verify LLDP configuration

***Procedure:***

* Go to the configuration terminal
  + config
* Enter the following commands

lldp-global-config msg-tx-interval 20

lldp-global-config tx-delay 3

lldp-global-config msg-tx-hold-multiplier 5 lldp-global-config admin-enabled true

lldp-global-config reinit-delay 1

* Go back out of configuration terminal

# exit

* Check the config changes
  + show lldp

You should see something like the following:

+------ LLDP GLOBAL CONFIG +

| Parameter | Value |

+ + +

| admin-enabled | True |

| msg-tx-interval | 20 |

| reinit-delay | 2 |

| tx-delay | 3 |

| msg-tx-hold-multiplier | 5 |

| notification-interval | 5 |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Built in Trial License

Trial License means a License granted to a User or an Organization for a limited duration (90 days), to enable the User or the Organization to evaluate the Software and to do demo of Software Trial Licenses are provided free of charge. This will help FSE and customer to

test devices/software without purchasing the actual license.

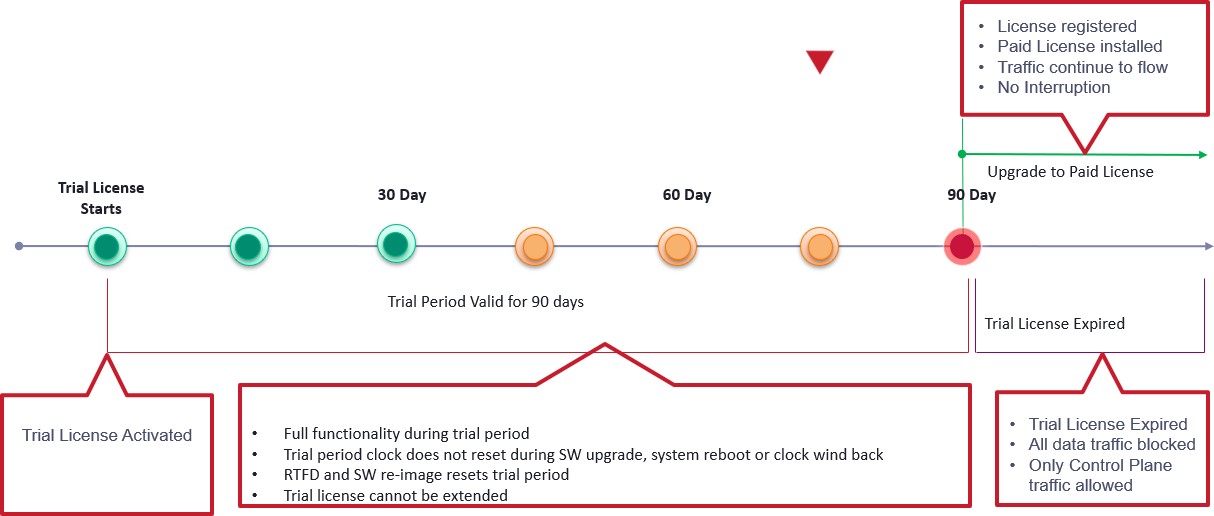
***Objective:***

In earlier releases (SAOS 10.4,SAOS 10.5) we do not have this functionaly. So in order to test device or software we need to register device and purchase license. But now in 10.6 build in trial license support come. A trial license in built come with software which just need to activate and its free. User can use this license for 90 days after that they have to purchage new trial license or permanent license.

On expiration of trial license all data traffic will be block but control traffic will work. User need to purchase license in order to continue services traffic.

Valcli command to activate license on device. Initially no need to download external license:

5164 > license activate built-in-trial-license



#### Functional Behavior

* Temporary, trial/evaluation licenses are built into SW across all Valimar product variants
* Valid only for fixed, pre-defined period (90-Days)
* Enables full feature functionality supported in that SW release for the trial period
* Built-in trial licenses are explicitly activated by user to start the 90-Day trial period
  + Trial period clock does not reset upon clock wind back or SW upgrade or system reboot
  + SW re-image or RTFD on the device will result in a new trial period
* Built-in trial license cannot be extended
  + Extending the trial /period requires a new trial license to be obtained from the portal and installed on the device
  + Moving to paid local(manual)license requires registering the device on the portal, mapping entitlements to device, generating device specific license file and installing it on the device. Once perament license insalled you can not use trial license after that.
* Built-in trial license cannot be extracted out of a SW instance and applied to elsewhere.
* Once the built-in license expires, traffic is blocked in the data plane ;control plane traffic is still allowed
* Acquisition of a paid license(local or server-based) will invalidate the built-in trial license even if the trial period has not expired.

**Note** Event/alarm notification for expiry of built-in license will trigger on 45, 30, 15, 7, 6, 5, 4,

3, 2, 1 day(s) before

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### System gNMI Alarm enhancements

***Requirement:***

* Prior to 10.7.1, the alarm inventory table will show the default severity against each alarm and any user change of severity against each alarm was not displayed.

***Objective:***

* From 10.7.1 onwards, the s/w will display default severity in Alarm Inventory and support Configurable alarm severity as per RFC 8632.
* For each alarm, a maximum of 4 operator state change and 16 system triggered state change history logs will be available for user reference.
* The user can now create multiple alarm shelves with different criteria. The permissible upper limit is 8 shelves.

***Procedure & Configuration:***

* Create alarm profile to configure severity levels of the alarms:
  + alarms alarm-profile <alarm-type-id> <alarm-typequalifier-match>

<resource> alarm-severity-assignmentprofile severity-level <severity- level> <severity-level> <severity-level>

* Configuring alarm history count:
* A. For system triggered alarm state change count:
  + alarms alarm-profile <alarm-type-id> ALL ALL max-alarm-status-changes

<count>

* B. For operator triggered alarm state change count:
  + alarms alarm-profile <alarm-type-id> ALL ALL max-alarm-operator-state- changes <count>
* Set the alarm operator state:
  + alarm set operator-state resource <alarm-resource> type <alarm-type> type-qualifier <alarm-type-qualifier> state <operator-state> text

<text>

***Configuration:***

5164> sh run sec alarms config

alarms control alarm-shelving shelf 'Fan-speed' alarm-type-id fan-max- speed alarm-type-qualifier-match "ALL" resource "r1"

alarms alarm-profile 'interface-fault' 'ALL' 'ALL' description "Test123" max-alarm-status-changes 14 max-alarm-operator-state-changes 3

alarms alarm-profile 'interface-fault' 'ALL' 'ALL' alarm-severity- assignment-profile severity-level critical

5164>

***Verification:***

5164> show alarm inventory alarm-type interface-fault

+

| Type

+

ALARM INVENTORY

| Qualifier | Severity | Description

+

+

+

+

|

+

| interface-fault | | critical | Interface oper state change |

+

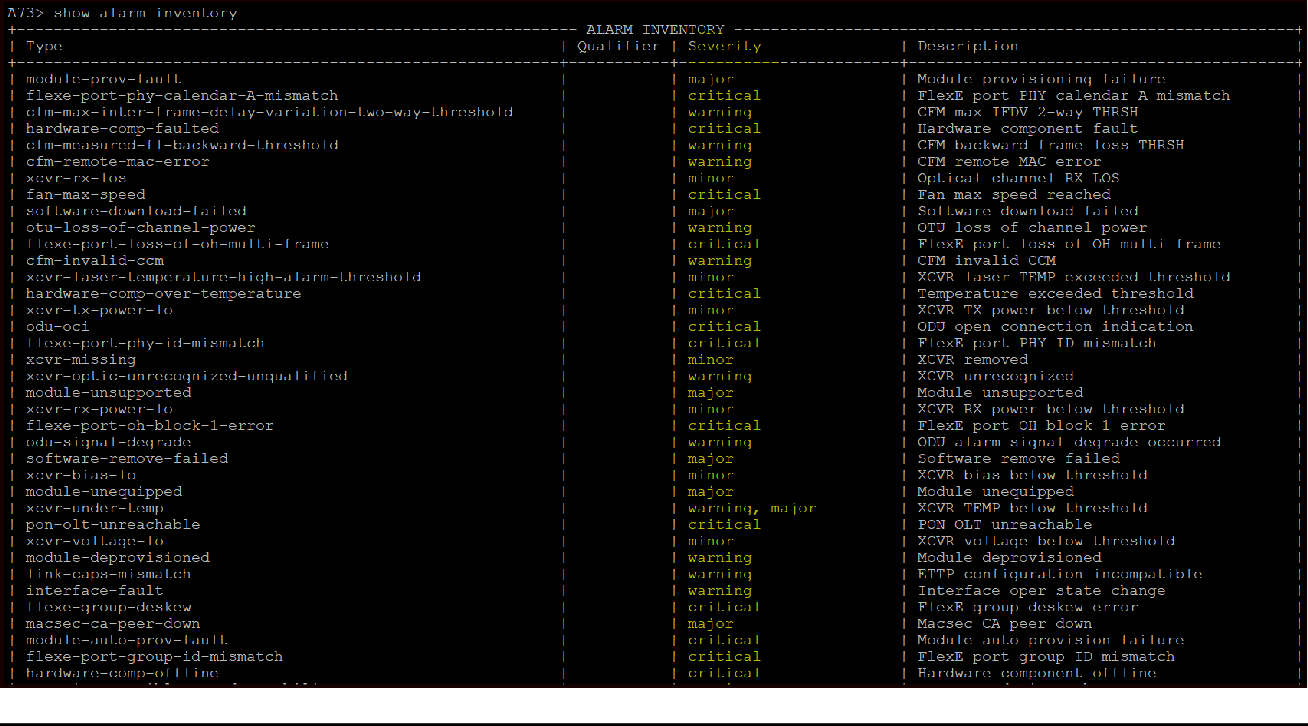
5164-201-A>

+

+

+

+



Test Case Results:

Passed: Yes No Verified by Date/Time Comments

## FRU

### 5171 – FRU

In 10.3, with the introduction of 5171, Field Replacement Unit insertion and removal are now supported on 5171. Only the 2xQSFP28 FRU is supported in 10.3.

In 10.4, additional FRU introduced for 5171 platform. FRU - 1xQSFP28+1xCFP2 and 2xQSFP28 is supported in 10.4 and onwards.

###### Insertion of a FRU

***Objective:***

Verify the insertion of a FRU.

***Procedure:***

* Insert the FRU into the 5171 first slot, and display status. FRU type will automatically get detected on the system
  + show system components component slot1

5171-A> show system components component slot1

+ COMPONENT: SLOT1 +

| Name | Value |

+ + +

| name | slot1 |

| type | openconfig-platform-types:MODULE |

| id | INUIAGTCAA |

| description | slot1 manufactured on 10092019 |

| serial-no | M96DA5A8 |

| part-no | 170-0315-900 |

| fru-type | CFP2-QSFP28 |

| admin-state | enabled |

| module-state | Up |

+ + +

5171-A>

* Display all components of 5171.
  + show system components

5171-A> show system components

+ PLATFORM INFO +

| Name | Value |

+ + +

| name | 5171 |

| type | openconfig-platform-types:CHASSIS |

| id | INMCR00DRA |

| description | 5171 |

| mfg-name | Ciena |

| version | 1 |

| serial-no | M96F06AB |

| part-no | 170-5171-900 |

| base-mac | 20:80:58:81:87:80 |

| status-led | solid-green |

| alarm-led | off |

| psa-led | off |

| psb-led | off |

+ + +

+------- PLATFORM: 5171 +

| Component | Present |

+ + +

| fan-board | yes |

| fan1 | yes |

| fan2 | yes |

| fan3 | yes |

| fan4 | yes |

| fan5 | yes |

| fan6 | yes |

| fan7 | yes |

| fan8 | yes |

| fan9 | yes |

| fan10 | yes |

| fan11 | yes |

| fan12 | yes |

| psu-board | yes |

| psa | yes |

| psb | no |

| cpu1-temperature | yes |

| cpu2-temperature | yes |

| front-temperature | yes |

| switch-temperature | yes |

+ + +

+

+

MODULES

| Slot | Configured-Fru-Type | Admin-State | Fru-Type | Module- State |

+ + + + +

+

| slot1 | CFP2-QSFP28 | enabled | CFP2-QSFP28 | Up

|

| slot2 | qsfp28 | enabled | qsfp28 | Up

|

+ + + + +

+

5171-A>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Enable FRU module using CLI

***Objective:***

Verify the insertion of a FRU and provision FRU-type manually

***Procedure:***

* Pre-provision the FRU type using the commands below, delete the already configured FRU if any

>config

#components component <slot> properties property fru-type config value none

* Configure QSPF28/CFP2 Combo FRU:

>config

#components component <slot> properties property fru-type config value <fru-type>

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Licence install - CFP2-DCO plugs

***Objective:***

Note that the data and time set is required for the application of the license. Below step is required to apply license to the installed CFP2-DCO plugs in combo CFP2-QSFP28 FRU. This will activate the features and ports will be controlled in SAOS 10.4 and onwards.

One CFP2-DCO license per CFP2 plug or per ETTP port is required

***Procedure:***

* Apply license server on configuration CLI. Internal Ciena server used below.

license-management-config license-client-config server- enable enabled

license-management-config license-server-config *10.182.34.96*

exit exit

* Insert CFP2-DCO xcvr on the FRU port

5171-A> show xcvr

+

+

XCVRS INFO

| Xcvr | Vendor Details | Connector Type | Admin State | Oper State | Mode |

+ + +

|

+ +-

| 1/1 | CIENA 180-2111-900 | LC | enabled | up

| 28-100 |

+ + + + +

+ +

* Configure service to send tagged/untagged traffic

>config

classifiers classifier VLAN100 filter-entry vtag-stack vtags

1 vlan-id 100

fds fd fd1 mode vpls fps fp fp1

fd-name fd1 logical-port 1/1.1

classifier-list VLAN100 classifier-list-precedence 1

mtu-size 2000

egress-l2-transform push-vid-100

vlan-stack 1

push-tpid tpid-8100 push-vid 100

* Once above 2 conditions met, device will auto fetch license from license server

>show license

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### Configure CFP2-DCO ports

***Objective:***

Configure CFP2-DCO ports.

***Procedure:***

* ***Prerequisites –*** device must have valid license and FRU should be in UP state
* Set frequency of the port

>config

#ptps ptp <slot/port> properties transmitter frequency value

<0.0 | 186087.5 .. 190956.2 | 191100.0 .. 196150.0 >

* Verify the port status

5171-A> show logical-ports logical-port 1/1.1

+---- LOGICAL PORT +

| KEY | VALUE |

+ + +

| Name | 1/1.1 |

| Ettp | 1/1.1 |

| Admin State | enable |

| MTU | 1526 |

| Description | 1/1.1 |

+ + +

+------- LOGICAL PORT STATE +

| KEY | VALUE |

+ + +

| Name | 1/1.1 |

| Index | 41 |

| Mac Address | 20:80:58:81:87:b2 |

| Oper State | Up |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time Comments

###### 5171 Front Temperature Sensor – Early Notification of High Temperature

***Objective:***

* + - * Verify that early notification alarm for high temperature threshold crossing is working. This testcase only applies to 5171 front temperature sensor.

Pre-requisites:

* + - * 5171 running SAOS 10.7.1 or later.
      * 20C below the max-temp-threshold would raise an early notification warning
      * 10C below the max-temp-threshold would raise a major early notification warning
      * When max-temp-threshold is crossed, a critical alarm is raised.

***Procedure:***

* + - * Display the current temperature threshold settings, and also the instantaneous temperatures on 5171 as monitored by the front temperature sensor.

5171\_0042> show system components component front-temperature

+------------- COMPONENT: FRONT-TEMPERATURE +

| Name | Value |

+ + +

| name | front-temperature |

| type | openconfig-platform-types:SENSOR |

| instant | 32.0 C |

| avg | 32.0 C |

| min | 32.0 C |

| max | 33.0 C |

| max-temp-threshold | 65.00 C |

| min-temp-threshold | -40.00 C |

| state | Ok |

+ + +

* + - * Enable alarm early notification :

config

components component front-temperature properties property alarm-early-notification config name alarm-early-notification value enabled

* + - * Configure the max-temp-threshold to 45C.

config

components component front-temperature properties property max- temperature-limit config name max-temperature-limit value 45

* + - * Display the front temperature

CN5171\_0040> **show system components component front-temperature**

+ COMPONENT: FRONT-TEMPERATURE +

| Name | Value |

+ + +

| name | front-temperature |

| type | openconfig-platform-types:SENSOR |

| instant | 33.0 C |

| avg | 32.0 C |

| min | 32.0 C |

| max | 33.0 C |

| max-temp-threshold | 45.00 C |

| min-temp-threshold | -40.00 C |

| max-operating-temp | 65.00 |

| min-operating-temp | -40.00 |

| state | Ok |

| alarm-early-notification | enabled |

+ + +

* + - * Display alarm – expectation is that a Warning alarm is raised when temperature of device crosses 25C. ie: 20C below the max-temp-threshold
      * Next set the max temperature threshold to 40C.



components component front-temperature properties property max- temperature-limit config name max-temperature-limit value 40

* + - * Display the temperature settings:

CN5171\_0040> show system components component front-temperature

+ COMPONENT: FRONT-TEMPERATURE +

| Name | Value |

+ + +

| name | front-temperature |

| type | openconfig-platform-types:SENSOR |

| instant | 33.0 C |

| avg | 32.0 C |

| min | 32.0 C |

| max | 33.0 C |

| max-temp-threshold | 40.00 C |

| min-temp-threshold | -40.00 C |

| max-operating-temp | 65.00 |

| min-operating-temp | -40.00 |

| state | Ok |

| alarm-early-notification | enabled |

+ + +

CN5171\_0040>

* + - * Display the alarms now, expectation is for a major alarm to be raised when the temperature crosses 35C ie: 10C below the max-temp-threshold



Test Case Results:

Passed: Yes No Verified by Date/Time

Comments

## Device Management

#### WebGUI

From SAOS 10.4 release and onwards, WebGUI for provisioning was introduced. The usage of the WEbGUI to create provisioning is very intuitive. It is a good alternative to using the CLI or NETCONF browser to provision a node. In the sections below, some basic provisioning testcases will be validated using the WebGUI.

###### WebGUI – Management of Sessions

***Objective:***

Validate WebGUI can be enabled and disabled. Please note that WebGUI is not supported on all platforms, for example 3926 and 3928 platforms do not support WebGUI.

***Procedure:***

* Display current web-gui state:

show web-gui state

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

| State | Disabled |

+ + +

* Enable Web GUI. This Web GUI can take a couple of minutes before it is fully enabled.

set web-gui state enable

* Display the Web GUI state again, after waiting for a couple of minutes.

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

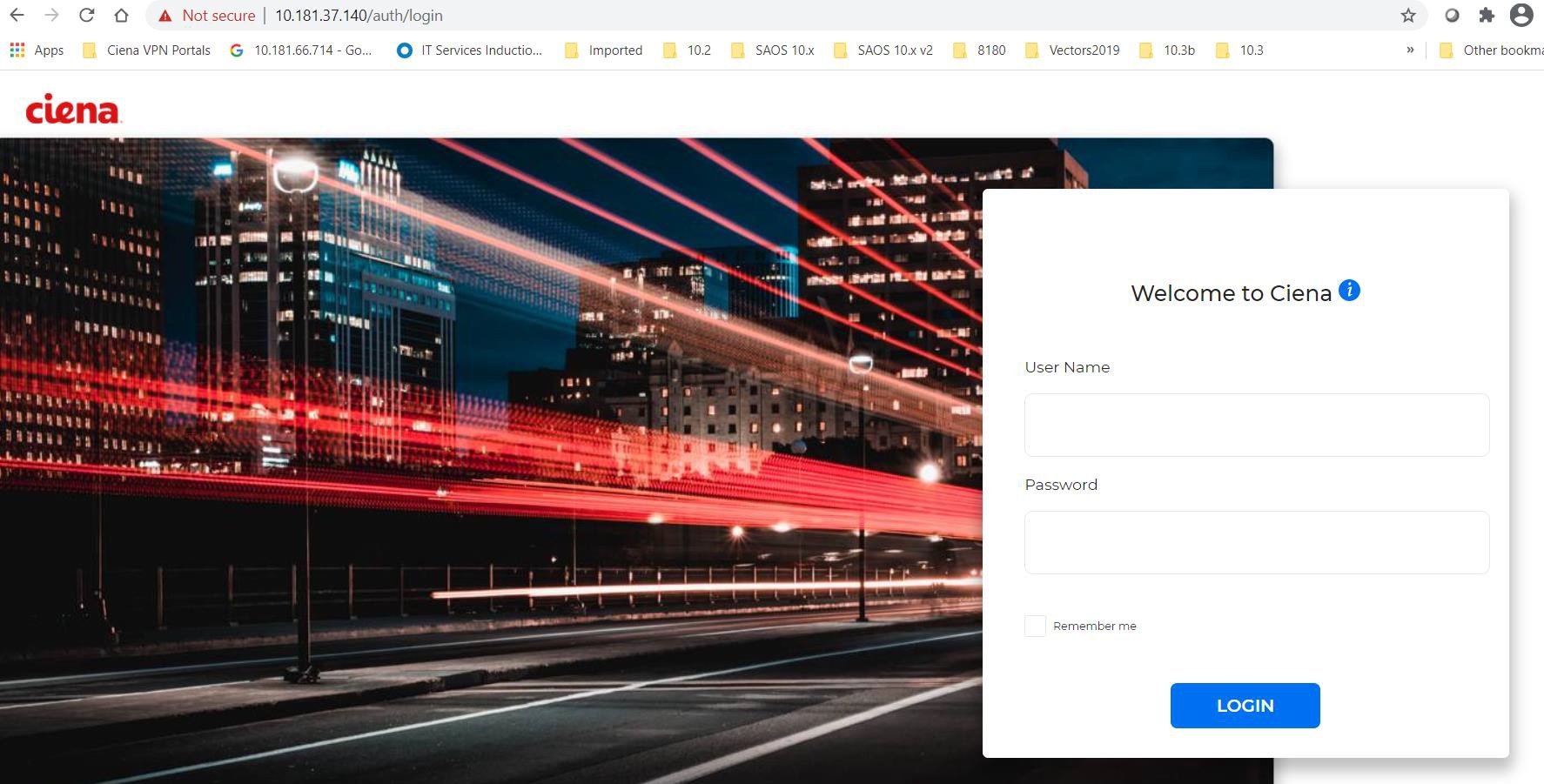
| State | Enabled |

+ + +

* Go to a web browser and enter the node’s IP address. This may take a few minutes before

the GUI becomes available.

Enter URL https://x.x.x.x/



* Login using default or created user account – default is : **diag/ciena123.** Wait for GUI to launch. This may take a few minutes.
* Display the webUI sessions on the CLI. Up to 3 concurrent sessions are supported. Show web-gui session

5166-004> show web-gui session

+ WEBGUI SERVER SESSIONS +

| ID | Client | User | Last Access |

+ + + + +

| 1 | 169.254.160.50 | diag | 2020-12-16 07:22:14 PM |

+ + + + +

* Use the following command to kill a session. **unset web-gui session id 1** 5166-004> unset web-gui session id 1

+ WEBGUI SERVER SESSIONS +

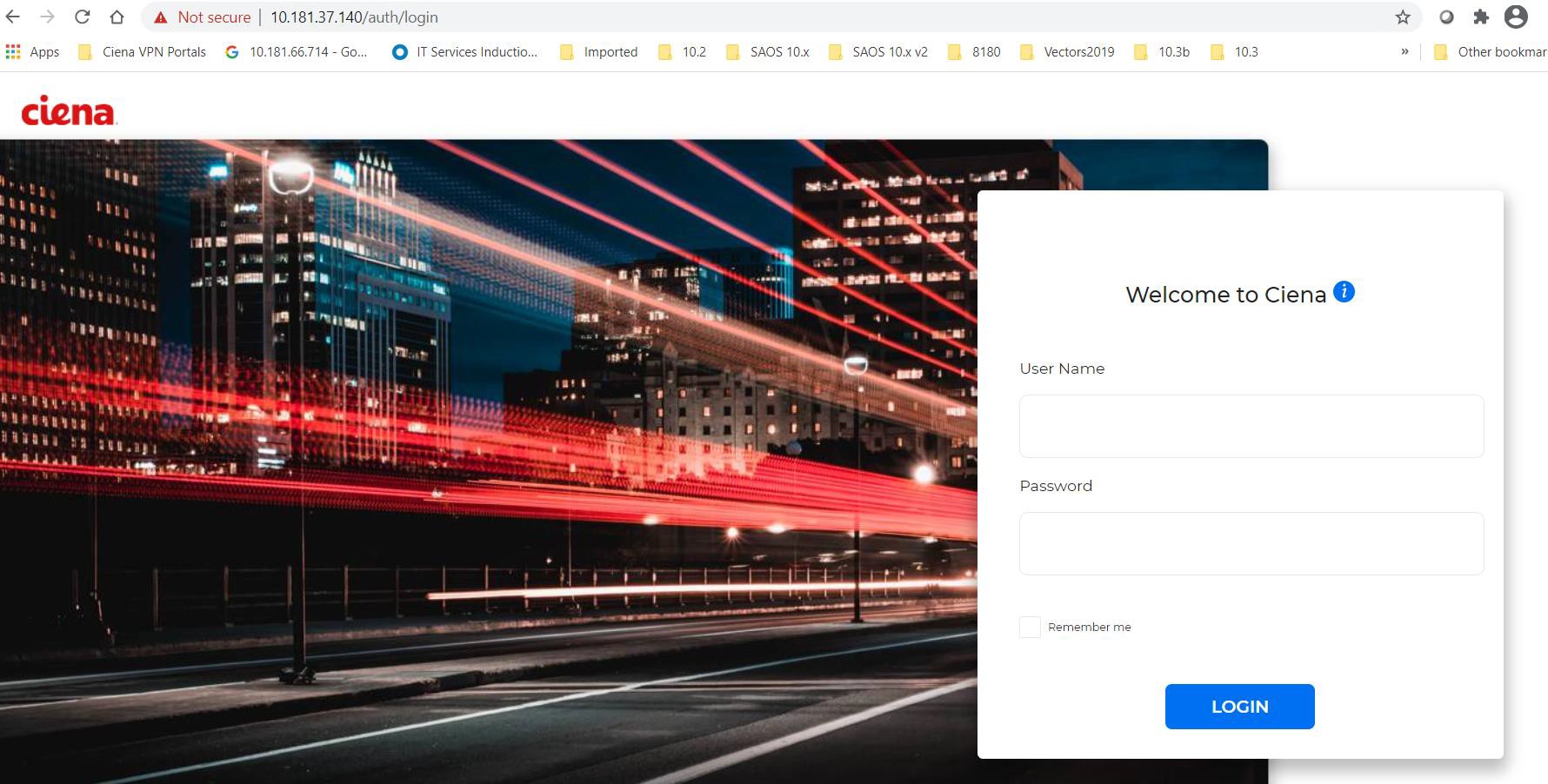
| ID | Message |

+ + +

| 1 | User ID 1 killed. |

+ + +

The webGUI session was logged out.



* To disable the web GUI, enter the following command :

set web-gui state disable

* Display the state of the WEB GUI to ensure that it is disabled.

show web-gui state

5166-004> show web-gui state

+----- WEBGUI +

| Name | Value |

+ + +

| State | Disabled |

+ + +

Test Case Results:

Passed: Yes No Verified by Date/Time

Comments

\*\*For more WebGUI examples, please see Appendix A.