Release Notes for Cisco NCS 2000 Series, Releases 11.12 and 11.1.2.3

First Published: 2021-08-06

Last Modified: 2023-06-26

Cisco NCS 2000 Series Release Notes

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

This Release Notes document contains information about new features and enhancements, in the Cisco platforms.

Software and Hardware Requirements

Before you begin to install the software, you must check whether your system meets the following minimum software and hardware requirements:

- Hardware—Intel Core i5, i7, or faster processor. A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.
- One of the following operating systems:
  - Windows 7, Windows Server 2008, or later
  - Apple Mac OS X
  - UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.
  - Ubuntu 12.10
- Java Runtime Environment—JRE 1.8 and later.
- Java version 8.0
- Browser:

- Internet Explorer
- Mozilla Firefox
- Safari
- Google Chrome

Changes in Release 11.1.2.3

Cisco is continuously enhancing the product with every release and this section covers a brief description of changes in this release.

TACACS Idle Timeout Considerations:

- From release 11.1.2.3, the TACACS server sends the idle timeout value in the minutes. Previously the unit for idle timeout value was seconds. After you upgrade to release 11.1.2.3, the idle timeout value unit gets adjusted to minutes from seconds.

  Example: On the TACACS server, the idle timeout value of 900 seconds gets changed to 900 minutes after you upgrade to release 11.1.2.3.

- The default idle timeout value on the TACACS server is 60 minutes. If you set an idle timeout value on the ISE/ACS TACACS server, the TACACS authenticated sessions expire when the idle timeout value is reached. However, if the CTC client is active after the idle timeout has expired, the CTC session remains open.

Caveats

Open Caveats in Release 11.1.2.3

The following table lists the open caveats:

Identifier	Headline
CSCwb66820	Random traffic errors on 400G-XP clients when connected to a 10x10G-LC CXP Fanout
CSCwb63907	HI-LASERTEMP alarm on the CXP ports of a 10x10G-LC
CSCwa91226	NCS2K ONS-SC-OSC-18.0= pluggable RX power range [-22.8dBm, -50dBm] due to h/w limitation
CSCvw49760	RAMAN need alarm raised during abort if no pump on
CSCwb44954	Active login showing junk IPV4 ip when CTC launched with IPv6 ip
CSCwb35138	TL1 does not support for adding Multiple REGEN Constraints
CSCwa87699	TNCS2/TNCS2O: Post switchover ending with CONTBUS reported by LCs and EMS port down state

Identifier	Headline
CSCwb76743	No pop-up or event has been sent when "Notify when completed" flag is selected

Resolved Caveats in Release 11.1.2.3

The following table lists the resolved caveats:

Identifier	Headline
CSCwb10645	Unclear error message trying to create IPC with LMP present
CSCvy24166	10x10G-LC, 10Ge to OTU2e CBR transponder mode configuration, latency variation improvement
CSCvy79016	passive device connected to SSC with TNCS-2 TNCS-2O disappear while activating 11.1.2
CSCwb14928	Unwanted prints on Controller while collecting diagnostics logs when Temp.PTB is "0" size.
CSCvz76849	400G-XP: FEC PM Uncorrectable Words counter remain valid during fiber cut
CSCvw97478	tCPReq keepAlive failure or cold reset in case of RTXP on LAN
CSCvy35710	[CPAK-FR-S]: Discrepancy in actual eqpt type in CTC and TL1 for CPAK-FR-S
CSCwb56922	Refresh button under optics PM is not working after Pluggable port creation/deletion on 10x10G
CSCwb55266	NCS2000: Secure TL1 - Flow control improvement at SSH
CSCvz09027	PARAM-MISM condition configuring Gain Degrade Thresholds higher than 30dB
CSCwb11002	TL1 Unclear error message trying to create IPC with LMP present
CSCwa24019	User unable to login to node via TL1/Vxworks and ExcTask in suspended state
CSCwb71185	M12 nodes crashing with tSshd task exception
CSCvv40170	Pre-provisioned regen cards OR pre-prov REGEN card PPMs cause periodic node cold reboot
CSCwa73593	Version not updated in CTC Launcher
CSCvy51837	[Encryption]: KEY-EX-FAIL alarm on LCs when NE and FE are different releases
CSCvz60351	SMR20 card in 2nd Layer add/drop stage may remain with ALS enabled
CSCvz52384	KEY-EX-FAIL alarm on 400G-XP when NE and FE are different releases
CSCvv00112	CET: Node took autoreset on tNPRTask (deadlock by OTDRMgr in a specific scenario)
CSCwa82623	Node reset after sending RTRV-CPSRESTPATH TL1 command

Identifier	Headline
CSCwa26376	10x10G-LC card with FANOUT Mode fails to boot if the CXP is plugged in
CSCvu64436	Node hung with legacy Card (Non TNCS2/Non TNCS2O) - flooding of tNetTask wth netJobAdd continuously
CSCvy90108	After Downgrade both controller cards are in roll reboot
CSCvz65077	OBFL file is corrupted while writing logs to it
CSCvs28305	TNCS2O/TNCS2/TNCS/TNCO: CTC shows optical powers swapped on OSC current PM
CSCvz82717	SMR20 side card in 2nd Layer add/drop configuratio may not start APC regulation
CSCwb41677	TACACS superuser incorrect logged in as retrieval user
CSCwa49941	Reverted and activated circuits being deleted incorrectly because of preemption
CSCvv98192	Circuit down due to 200G regen trunk state change from OOS_MT to IS during circuit activation
CSCwa56195	Evaluation of CTC for Log4j RCE (Log4Shell) Vulnerability
CSCvw06490	Random traffic hits/OPR alarms seen on cckts spanning long smr-flex chains (more than ~12 SMR-FLEX)
CSCvz01455	CTC not able to discover nodes/links randomly - CORBA task struck in SSL_read
CSCwa70823	ONS-SC-OSC-18.0 SFP for RAMAN link reports incorrect OSC RX power
CSCvw76302	On executing active TNC MANRESET - Standby takes one autoreset / fails to takeover as new active
CSCvz30524	TNC switch/LC manreset with expired license leads to No relevant alarm/ silent trunk laser off
CSCwa33828	TNC crash at startup of CV
CSCvz55021	Data path goes down with INVALID-MUXCONF alarm when s/w upgrade is performed[11.12-F to 12.30-SSON]
CSCvx08604	SMR9/20: Random traffic hits on span seen due to OTDR scan/OSC LOS/Automatic OTDR training
CSCvv00564	OCH-TRAIL reverted to main path but the circuit state stayed in ADMIN_OOS_DSBLD
CSCwb35129	TACACS authenticated TL1 sessions closed at different timeout value instead of actual value set
CSCvz76622	TL1 response of rtrv-CPSRESTPATH::ALL:123; is having ??? for a restored Remote txp circuits
CSCwa70609	[SRC][CT1881]SecurityControlError: Certificate lifetime should not exceed 5 years

Identifier	Headline
CSCwb34989	[MR-MXP]:FPGA upgrade operation with no FPGA change image is causing hard reset on card
CSCwb08798	Restored circuit does not use the regenerator of the main circuit
CSCvw07940	TACACS Idle Timeout not working and excessive high stale users present
CSCvy42283	NCS2006: In NCS2K network regen(NCS1004) is not selected correctly by media channel(MCH)
CSCwb41155	ent-mch erroneously requires the user/machine to use uppercase characters for the tail-end MPO AID
CSCvt18849	[CTC]:Inconsistent optics PM values for payload provisioned under SR PPM on MR-MXP card
CSCwb16732	GMPLS resignal retry interval for external trunk continuosly increase when trunk is admin down
CSCvw57946	TNCS2O FRCD reloaded with error "Data buffers percentage critical: 19% free", R11.12, Build-19
CSCvs11669	SSH CTR cipher not working
CSCvx16952	Pt to pt wson circuit goes stuck in restoring state (during restore) if restore constrnts reversed
CSCvw56996	Task CORBA blocked waiting on ssl connection socket preventing CTC sessions to open
CSCvz05698	CV does not verify some patch-cords if there is a RAMAN card present in the node
CSCvu28030	Regen node TNCS/TNCS-O resets during WSON circuit signaling
CSCvz56797	[TNC]: Controller card went for a task while performing license rehost operation
CSCvz14082	IPC creation is allowed when the LMP is active with TXPCONTROLMODE=GMPLS.
CSCvy89029	M12: During Upgrade I/O cards are reporting Fake alarm "COLD-RESTART" Instead of AUTO-RESET
CSCvy65667	[MR-MXP]:Sometime FPGA upgrade failed on MR-MXP card and card is going for crash
CSCwb00448	PPM High Power/FW Upgrade Failure after the upgrade from Rel 11.112
CSCvy15822	ACT/SBY Controller tHwHiPriPoll exception reset seen randomly
CSCvy69186	TNC randomly need 10+ minutes to switchover
CSCwb38410	[MR-MXP]:Some time FPGA upgrade operation causes SOFT-VERF-FAIL on MR-MXP card
CSCwb02021	Circuit not restored in presence of APC_DISABLED alarm on the shortest path

Identifier	Headline
CSCwb26280	11.123:Copy rights of CTC debug window showing as 2000-2006 only, need to correct it
CSCvz52382	KEY-EX-FAIL alarm on Mr-Mxp when NE and FE are different releases

Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

What's New in Release 11.12

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements. It also includes links to detailed documentation, where available.

Feature	Description
Control Card and Node Configuration	
Fiber Shuffle Upgrade	This feature allows you to upgrade the Boot ROM version, OS Kernel, and Uboot version of the fiber shuffle through CTC.
Line Card Configuration	
Dynamic Power Allocation on 200G-CK-LC and 400G-XP-LC Cards	This feature allows you to dynamically allocate power based on the line card operating mode. This maximises the usage of the NCS 2015 chassis slots in a 2+2 PSU configuration.This feature is supported on the 200G-CK-LC and 400G-XP-LC cards.
Secure Unique Device Identification (SUDI) SUDI 2099 Certificates for WSE, MR-MXP, and 400G XP Cards	This enhancement allows you to extend the usage of WSE, MR-MXP and 400G-XP-LC cards with encryption functionality beyond year 2029. This extended validity helps to avoid encryption and card upgrade failures. The existing SUDI 2029 certificate allows the user to have encryption functionality only for ten years from the card installation or until 2029 whichever is earlier. This enhancement to include SUDI certificate 2099 on the software allows the user to extend the usage of encryption functionality up to year 2099. Both the near-end and far-end nodes must use the same SUDI certificate.
Network Configuration	

Feature	Description
Custom Alien Wavelength and MEDIA CHANNEL OCH NC circuit management through CTC	The feature allows you to create an MCH custom alien wavelength and the associated MEDIA CHANNEL OCH NC circuit specifying the following parameters through CTC: • Signal width • Modulation guard band • Filtering guard band This functionality enables you to create a medial channel of any spectrum size, for example, signal width of 34.20 GHz, modulation GB of 1.71 GHz, and filtering GB of 4.92 GHz.
ZR+ configuration support on NCS 2000 with 6AD passive add or drop in colorless configuration.	The following two alien wavelengths are supported in R11.12: • QSFP-DD-ZR • QSFP-DD-ZR+
Installing the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms	
Pluggables Support	• QSFP-100G-FR-S pluggable is supported on 400G-XP-LC card. • CPAK-100G-FR pluggable is supported on 200G-CK-LC and MR-MXP cards

TLS Version Support

The supported version of Transport Layer Security (TLS) protocol is 1.2.

Caveats

Open Caveats in Release 11.12

The following table lists the open caveats:

Caveat ID Number	Description
CSCvy49234	400G-XP-LC: Link error during auto switch for 100GE payloads on FR-S pluggable with squelch as `LF`.
CSCvy51837	[Encryption]: `KEY-EX-FAIL` alarm on LCs when NE and FE are different releases.
CSCvy61787	[EDVT 200G-CK-C+MR-MXP]: Traffic errors from CPAK-FRS (Tx side) on Titano 3 after node Power Cycle.

Caveat ID Number	Description
CSCvy61795	[EDVT 200G-CK-C+MR-MXP]: Traffic errors from CPAK-FRS (Tx side) on Falco after node Power Cycle.
CSCvy65667	[MR-MXP]: Tyler FPGA upgrade fail on MR-MXP card.
CSCvx09244	CTC show NCS2k node with `Activating` pop-up even if the operation completed.
CSCvx29636	TL1 output for OPWR is wrong for RAMAN interfaces.
CSCvx60735	CTC disconnected and fail to reconnect.
CSCvy43195	Signal Width, Modulation GB and Filtering GB should be filtered for `OCHCC/OCHTRAIL/CARRIER`.
CSCvy46793	CTC - Minimum required characters are not taken into account while evaluating the password change.
CSCvy53238	400G-XP-LC: Link error is displayed during trunk terminal loopback on FR-S pluggable with Squelch as `LF`.
CSCvy53260	400G-XP-LC: CTC:OCH port listing is present for 100G-QSFP-FR-S pluggable under Optics Threshold which must be removed.
CSCvy58760	FS firmware upgrade fails on TNCS-2 TNCS-2O cards.
CSCvy69171	TNC does silent reboot 3 minutes after switchover.
CSCvy69186	TNC randomly need 10+ minutes to switchover.
CSCvy69329	400G-XP-LC: Traffic does not recover on E2E Setup with FR-S on one end and SMSR on the other end in some cases with physical loopback.
CSCvy75765	MR-MXP: UNC-WORD events report for OTU2 payload upon LC warm reboot.
CSCvy79016	Passive device connected to SSC with TNCS-2 TNCS-2O disappear while activating 11.12.
CSCvy89029	M12: During upgrade, I/O cards report fake alarm COLD-RESTART instead of AUTO-RESET.
CSCvz14082	IPC creation is allowed when the LMP is active with `TXPCONTROLMODE=GMPLS`.

Caveat ID Number	Description
CSCvz11616	Attempting to edit the TXPCONTROLMODE from Local to None and vice versa from TL1/CTC is not allowed.

Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Other Important Information and References

Alarms

The following alarm is added:

- ENC-CERT-EXP

Documentation Roadmap

Use the documentation roadmap to quickly access publications of Cisco NCS 2000 Series, Release 11.x.x
https://www.cisco.com/c/en/us/td/docs/optical/r11/ncs/doc-roadmap-ncs/b-ncsroadmap-11xx.html

JRE Compatibility

The JRE Compatibility table displays the JRE compatibility with NCS 2000 software releases.

Supported Pluggables

The document at the following URL lists the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP, and CPAK modules that are supported on the Cisco NCS 2000 series platforms:

http://www.cisco.com/c/en/us/td/docs/optical/spares/gbic/guides/b_ncs_pluggables.html