Release Notes for Cisco NCS 2000 Series, Release 11.1.4 and 11.1.4.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco NCS 2000 Series, Release 11.1.4 and 11.1.4.1 3
New software features 3
New hardware features 4
Resolved issues 5
Open issues 6
Compatibility 6
Related resources 7
Legal information 8

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco NCS 2000 Series, Release 11.1.4 and 11.1.4.1

This Release Notes document contains information about new features and enhancements, in the Cisco NCS 2000 Series platforms.

For the latest version of the Release Notes for Cisco NCS 2000 Series, visit this URL: http://www.cisco.com/c/en/us/support/optical-networking/network-convergence-system-2000-series/products-release-notes-list.html

Important note

Starting with Release 11.1.4, ONS 15454 M12 chassis and TCC3 card are not supported on the ONS 15454 DWDM and WSON software packages. You must not attempt to upgrade ONS 15454 M12 nodes from a previous release to Release 11.1.4.

Changes in Release 11.1.4.1

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

- Added New software feature for Release 11.1.4.1
- Added Resolved issues for Release 11.1.4.1
- Added Open issues for Release 11.1.4.1

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for NCS 2000, Release 11.1.4.1

Product impact	Feature	Description
Software Reliability	Message Authenticator enablement in RADIUS Server configuration	A new configurable option **Enable Message Authenticator** is introduced in RADIUS Server to facilitate the validation of message authenticators in RADIUS responses. Additionally, these TL1 commands are enhanced to support this attribute from the TL1 interface: • RTRV-AAASERVERAUTH • ED-AAASERVERAUTH

Table 2. New software features for NCS 2000, Release 11.1.4

Product impact	Feature	Description
Software Reliability	LMP support for new DWDM interfaces	This release introduces the CIM8-C and CIM8-CE models as the new alien wavelength profiles. The new alien profiles use the NCS 1014 transponders to send and receive data up to 800G in the NCS 2000 network. The NCS 1014 transponders that support the CIM8-C and CIM8-CE alien wavelength are: • NCS1K14-2.4T-K9 The new profiles support these pluggable modules.

© 2026 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		• CIM8-CE-K9 • CIM8-C-K9
Software Reliability	OpenJDK support for CTC	From Release 11.1.4, CTC supports OpenJDK version 8 and later, an open-source software platform that offers several key advantages, including reduced licensing costs, and enhanced compatibility with modern Java applications. This transition ensures that CTC users benefit a cost-effective, and future-ready environment.
Software Reliability	Support for 32-channel passive filters	The NCS 2000 device now supports these passive filters. • NCS1K-MD-32E-CE • NCS1K-MD-32O-CE
Ease of Use	Scroll Bar Support for LMP List	A scroll bar now appears in the NFV when you right-click a node and select an option to view the regen list, ensuring the entire list is fully visible and easy to navigate. This enhancement improves accessibility and usability when working with long LMP lists.
Software Reliability	TACACS server support using TL1	TACACS server configuration is supported through CTC. TL1 now supports TACACS server configuration. This enhancement allows Network Management Systems (NMS) to configure TACACS for authentication and user profiles when accessing network elements. These new TL1 commands enable TACACS server configuration: • ENT-TACACSSERVER • ED-TACACSSERVER • RTRV-TACACSSERVER • DLT-TACACSSERVER
Software Reliability	SSH and SSL Upgrade	When you upgrade to R11.1.4, the SSH and SSL libraries upgrade to the latest revisions that provides better security, addressing vulnerabilities. New versions CTC supports after upgrade (R11.1.4) CISCOSSL: 1.1.1y.7.3.377 (6/6/2024) CISCOSSH: 1.14.55
Software Reliability	TL1 command for SMR20 FS Firmware Upgrade	The SMR20 FS line card now supports direct firmware upgrades through a new TL1 command. This allows users to trigger these upgrades directly from their automation platforms. New TL1 command introduced: FPGA-UPGRADE

New hardware features

This section provides a brief description of the new hardware features introduced in this release.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 3. New hardware feature for NCS 2000, Release 11.1.4

Product impact	Feature	Description
Hardware Reliability	CIM8 Alien Profile Support for NCS 1014 and NCS 2000 Integration	You can now manage end-to-end optical circuits for an NCS 1014 node through an NCS 2000 node using the new CIM8-C-K9 and CIM8-CE-K9 alien profiles. When you operate the NCS 1014 node with the NCS1K14-2.4T-K9 line card, you can select the options from the "**Alien Wavelength**" drop-down list: • CIM8-C-K9 • CIM8-CE-K9

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 4. Resolved issues for NCS 2000 Series, Release 11.1.4.1

Bug ID	Description
CSCws50436	Node Controller falls into roll reboot on upgrading to 11.14 on tSnmpd Task Exception
CSCws82335	11.14: SSH Login fails when the " Enable Shell Password" is set
CSCwt23802	NCS2K node lands into roll reboot if radius server does not include message authenticator in response
CSCwt05367	Memory Leak observed in encryption sub system

Table 5. Resolved issues for NCS 2000 Series, Release 11.1.4

Bug ID	Description
CSCwm33240	Evaluation of Network Convergence System 2000 Series for BlastRADIUS vulnerability
CSCwh70225	Inconsistency in OTU port name configuration from TL1
CSCwi03896	NCS 2000: Node stops connecting via TL1/EPNM/CTC with Radius Session limit reached Error
CSCwk38324	NCS 2000: Radius packet limit reached errors issue and associated debug logs enhancement
CSCwe96716	HTTP task stuck in socket read call due to protocol violation by peer.
CSCwm39697	CTC freezing or getting stuck randomly during normal operations

© 2026 Cisco and/or its affiliates. All rights reserved.

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 6. Open issues for NCS 2000 Series, Release 11.1.4.1

Bug ID	Description
CSCws95644	The diagnostics logs for the maintenance user node are incomplete from the CTC
CSCwt05085	TNCS2O card is not showing faceplate and observing Prov-mismatch alarm after migration from TNCSO

Table 7. Open issues for NCS 2000 Series, Release 11.1.4

Bug ID	Description
CSCwp23624	10Gige (GFP) Facility Loopback datapath errors detected on 10x10G Card
CSCwq30865	Circuit Signal Flow is not visible in CTC NFV
CSCwq30884	Signal width, modulation, and filtering values for the circuits are missing in CTC NFV.
CSCwq38499	Unexpected or irrelevant logs are being printed on the controller console
CSCwq39363	While performing a simultaneous download, slowness in download speed was observed in one of nodes
CSCwq44263	Missing entry in the Audit Log for the Activate operation
CSCwq52142	NFV link Missing for IPC which was created between 4x4COFS/MD-48 and TXP cards
CSCwq52159	EDFA-17 Line-Tx to A/D port 4X4 COFS displays bidirectional link instead of unidirectional in NFV
CSCwq56926	After Circuit Repair, sometime CTC still show circuits REPAIR_NEEDED
CSCwq61514	Restart CTC after IP change before PPC repair
CSCwq72715	NFV and Passive cards panel correction required for MD-32E-CE and MD-32O-CE
CSCws50436	Node Controller falls into roll reboot on upgrading to 11.14 on tSnmpd Task Exception

Compatibility

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

Hardware requirements

- Intel Core i5, i7, or faster processor.

© 2026 Cisco and/or its affiliates. All rights reserved.

- A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.

Software requirements

- 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
- OpenJDK version 8
- Java version 8.0
- Browser:
  - Internet Explorer
  - Mozilla Firefox
  - Safari
  - Google Chrome

Related resources

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 pluggable

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.