

Release Notes for Cisco ONS 15454 DWDM, Release 11.1.3.x

First Published: 2023-06-16

Last Modified: 2024-08-07

Cisco ONS 15454 DWDM Release Notes, Release 11.1.3



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 ONS 15454 DWDM platforms.

For the latest version of the Release Notes for Cisco ONS 15454 DWDM, visit the following URL:

<https://www.cisco.com/c/en/us/support/optical-networking/ons-15454-series-multiservice-transport-platforms/products-release-notes-list.html>

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

Critical Bug Fix in Release 11.1.3.2

The following critical issues has been resolved in Release 11.1.3.2:

- Incorporate WSON disable on NCS2K node factory mode to avoid traffic loss.
- Clicking on Event Scan Report option on OTDR Node Controller causing active controller autoreset.
- Unexpected EOC-E alarm flaps seen on ROADM node frequently.
- NCS2K: Radius shared secret string on CTC displaying garbage characters more than 16 characters in length.
- TNCS-2 and TNCS-2O controllers myst2 partition is formatted with DOSFS 1.0 in 11.x and 12.x from MFG.
- Node loads revert DB upon simultaneous reset on the controller cards.
- HTTP task stucks in the read call on a socket when peer is violating protocol.
- The user-defined alarm profile does not persist with controller switchovers or the software upgrade.

Critical Bug Fix in Release 11.1.3.1

The following critical issue has been resolved in Release 11.1.3.1:

Carrier multilayer view does not display ports information in OCH Layer in the media channel node controller session and carrier node controller session circuit.

What's New in Release in CISCO ONS 15454, Release 11.1.3

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	

Feature	Description
Accessing the Controller Cards using Link-Local Address	You can now use the link-local subnet address to access and configure the controller cards. This approach is helpful when you do not have admin privileges to the laptop through which the controller card is configured. Ensure that the controller card and the laptop are on the same subnet.
Line Card Configuration	
WSE and 400G-XP-LC Encryption for Incorrect SUDI Certificates	With this enhancement, the system establishes the right Secure Unique Device Identification (SUDI) certificate combinations on 400G-XP-LC and WSE cards, which are referred to during configuring encryption applications. The check and alignment of certificates ensure users can configure encryption settings without errors and failures. The enhancement applies to both the 10 years and 99 years certificate validity types.
On-demand Firmware Upgrade of SMR20 FS and SMR20 FS CV Cards	It is necessary to perform a firmware upgrade to clear the TRAF-AFFECT-RESET-REQUIRED (Traffic Affecting Reset Required) alarm on the SMR 20 and SMR 20 FS CV cards. The FIRMWARE Upgrade button has been introduced in the Maintenance > Firmware tabs to initiate the upgrade operation on demand. This button performs an instantaneous firmware upgrade to the latest version.
New PRBS pattern support for 400G-XP-LC card	CTC now supports INVERTEDPRBS_31 as one of the PRBS patterns that are used to perform data integrity checks on the encapsulated packet data payloads. When a network comprises of both NCS 2000 and NCS 1004 nodes, this enhancement facilitates interoperability between the 400G-XP-LC card and NCS1K4-OTN-XP cards, as the latter only supports INVERTEDPRBS_31 pattern.
Improved CSR encryption using RSA-4096	The 400G-XP-LC, WSE, and MR-MXP cards now support RSA-4096 for Certificate Signing Request (CSR) encryption. As the RSA-4096 uses a longer encryption key compared to previously supported RSA-2048 and RSA-3072, it improves the security level of the signed certificate.
Network Configuration	
Bright ZR+ and CFP2-DCO Configuration Support on NCS 2000.	This release introduces the Bright ZR+ and CFP2-DCO alien profiles to enable end-to-end optical circuit management of an NCS 1004 node through an NCS 2000 node. These profiles are used when the NCS 1004 node is operationalized with NCS 1004 QXP and OTN-XP cards. You can choose <i>ONS-CFP2D-400G-C-FOiC</i> or <i>DP04QSDD</i> from Alien Wavelength drop-down list to utilize these profiles. The DWDM trunk pluggable on NCS 2000 node supporting the new alien profiles are: <ul style="list-style-type: none"> • CFP2-DCO (ONS-CFP2D-400G-C-FOIC): <ul style="list-style-type: none"> • ONS-CFP2D-400G-C • DP04-CFP2-M25-K9 • Bright ZR+ (DP04QSDD): <ul style="list-style-type: none"> • DP04QSDD-HE0 • DP04QSDD-HK9 • DP04QSDD-LK9

Feature	Description
Hardware Installation	
New Modular DC Power Module for M2 Chassis	The design of the DC Power module is enhanced to make the power system modular. The modular units comprise a primary frame and two replaceable DC PSUs (available for both ETSI and ANSI variants), each with unique PIDs. The PSUs are field replaceable and provide redundancy to the power system.
Security Reference	
Improved network security using ACL	Using Access Control List (ACL), you can introduce an extra layer of security to NCS 2000 networks. Only the IPs approved by the network admin, which are included in the ACL, will get access to a node or a group of nodes in the network. This added security prevents unwanted machines or malicious hosts from logging into the NCS 2000 networks via CTC, TL1, Telnet, or SSH.
Security User Profiles on TACACS	This release introduces the “SECURITY USER” and “SECURITY SUPER USER” user profiles, which TACACS Authentication validates. These users get the privileges to perform encryption configurations on the device. This feature allows TACACS+ enabled users to perform encryption functionalities on WSE, MR-MXP and 400G-XP-LC cards of NCS 2000.
Pluggables	
QSFP-100G-ERL-S Pluggable Support	This release introduces support for the QSFP-100G-ERL-S pluggable. It provides 100GE client-side interface support for up to 25 km over a standard pair of G.652 Single-Mode Fiber (SMF) with duplex LC connectors. Currently, the QSFP-100G-ERL-S pluggable is supported on the 400G-XP-LC card.
TL1 Guide	
Accessing and Configuring the Controller Cards Using TL1	You can use the link-local subnet address to access and configure the controller cards when you don't have administrative access to the laptop, which is under the same subnet as the controller card.
SSON MCH Guardband Tuning to Force Larger Spectrum Allocation	Using the ENT-MCH service creation command, you can extend the default channel width allocated by the GMPLS control plane for the SSON MCH circuits to 100 GHz. For channel width extension, specify an appropriate value for these parameters through the TL1 command during the MCH circuit creation: <ul style="list-style-type: none"> • GUARDBANDMODULATION • GUARDBANDFILTERING

NCS 2000 to NCS 1010 Network Migration

This feature allows you to migrate from ONS15454 MSTP networks comprising of 80-WXC-C ROADM cards to NCS 1010 networks. This network migration enables fiber reutilization to achieve higher bandwidth and potentially expand to the L-band part of the spectrum. The TAC team will support to complete this migration procedure.

You can reach out to the TAC team by either logging into the Technical Support Website at <http://www.cisco.com/c/en/us/support/index.html> or contacting the Cisco Technical Assistance Center (1 800 553-2447).

TLS Version Support

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

Other Important Information and References

Alarms

The following alarms are introduced:

- [LOGIN-FAIL-ACL-FAIL](#)
- [USB-EMPTY-CODE-VOL](#)
- [NO-VALID-USB-DB](#)

TL1 Commands

The following new commands are added:

- DLT-ACL
- ENT-ACL
- RTRV-ACL
- SET-ACLCONFIG

Documentation Roadmap

Use the documentation roadmap to quickly access publications of Cisco ONS 15454 DWDM, Release 11.x.x <https://www.cisco.com/c/en/us/td/docs/optical/r11/dwdm/doc-roadmap-ons/b-onsroadmap11xx.html>

JRE Compatibility

The [JRE Compatibility](#) table displays the JRE compatibility with ONS 15454 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 ONS 15454 platforms:

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

Caveats

Open Caveats

The following table lists the open caveats:

Identifier	Headline
CSCwf12256	OTUK-TIM alarm severity to not changing to Critical post y-cable config deletion.
CSCwe26519	Not able to Apply/View xml from CTC Node view
CSCwf21063	Cold/Warm Restart may occur after INIT-SYS on Active Controller
CSCwe61213	[ECU]: IMPROPRMVL alarm is getting raised and cleared while plugging in the ppm in the ECU ports
CSCvz13169	CTC reconnect issue after ncs2k node disconnect due to crash / WD / missed keep alive
CSCwk11860	ACL host list for one node is showing in another node post Refresh in security super user panel
CSCwk11892	ACL host list for one node is showing empty list when in another node toggle b/w IPV4 & IPV6 in ACL
CSCwk38324	NCS2k : Radius packet limit reached errors issue and associated debug logs enhancement
CSCwk52351	Software download through TL1 cmd got failed for ENE devices under 11.132
CSCwk11601	Sometime Radius-enabled ENE device is not connecting , it shows an error: RAD_SERVER_FAIL_ERR in con
CSCwk55910	Traffic outage post OSC & IPC deletion on Sh-2 followed by fiber activity
CSCwk55982	EPNM7.1.3: Discovered OCH-NC WSON circuit is showing \"W\"&\"WR\" even though \"WR\" constraint not added.
CSCwj98017	[11.132]:Diagnostic log collection is taking very long time(~15-16min)
CSCwk11627	Refresh should be active for ACL panel superuser in node view in CTC
CSCwk28612	Debug logs enhancement to enable saving logs prior to system going for cold reboots

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.

Using Bug Search Tool

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Procedure

- Step 1** Go to the <http://tools.cisco.com/bugsearch>.
- Step 2** Log in using your registered Cisco.com username and password.
The Bug Search page opens.
- Step 3** Use any of these options to search for bugs, and then press Enter (Return) to initiate the search:
- To search for a specific bug, enter the bug ID in the Search For field.
 - To search for bugs based on specific criteria, enter search criteria, such as a problem description, a feature, or a product name, in the Search For field.
 - To search for bugs based on products, enter or select a product from the Product list. For example, if you enter “WAE,” you get several options from which to choose.
 - To search for bugs based on releases, in the Releases list select whether to search for bugs affecting a specific release, bugs that were fixed in a specific release, or both. Then enter one or more release numbers in the Releases field.
- Step 4** When the search results are displayed, use the filter tools to narrow the results. You can filter the bugs by status, severity, and so on. To export the results to a spreadsheet, click Export Results to Excel.
-