Release Notes for the Cisco Cloud Native BNG Control Plane, Version 2025.02.0

First Published: 2025-05-14

Cisco Cloud Native BNG Control Plane

Introduction

This Release Notes identifies changes and issues related to this software release.

Release Package Version Information

Software Packages	Version
bng.2025.02.0.SPA.tgz	2025.02.0
NED package	ncs-6.4.3-cisco-bng-nc-1.1.2025.02.0
NSO	6.4.3
NSO Core-Function-Pack	ncs-6.4.3-cisco-bng-smi-deployer-2025.02.0.tar.gz

Descriptions for the various packages provided with this release are available in the Release Package Descriptions, on page 5 section.

Verified Compatibility

This version of the cnBNG Control Plane has been verified with the following software components/packages. Consult the individual components/packages release notes for details.

Products	Version
BNG UP (ASR 9K)	IOS XR Release 25.2.1*
SMI CEE	2025.02.1.17
SMI Cluster Deployer	2025.02.1.17
SMI Base ISO Image	22.04.0-20250328

*Subject to feature availability.

What's New in this Release

New in Documentation

This version of Release Notes includes a new section titled **What's New in this Release** comprising all new features, enhancements, and behavior changes applicable for the release.

This section will be available in all the 5G release notes and will supersede content in the Release Change Reference (RCR) document. Effective release 2024.02, the RCR document will be deprecated.

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature	Description
RADIUS-Based Policing - QoS Shape-Rate parameterization	You can now dynamically manage your cnBNG subscriber services through RADIUS-based activation. With RADIUS-Based Policing (RaBaPol), you can customize service parameters, such as the QoS shape-rate, according to your requirements, giving you greater control over service management.
Shared Policy Instance	You can now allocate and share a single set of QoS resources across multiple cnBNG sub-interfaces and bundle sub-interfaces. By using a single QoS policy instance across multiple sub-interfaces, you can achieve aggregate shaping across your sub-interfaces, promoting streamlined bandwidth management.
Stateful-IPv6-Address-Pool support	We have enhanced IPv6 address allocation by enabling the RADIUS server to specify the assigned pool name to cnBNG. The cnBNG uses this information to assign IPv6 addresses to subscribers.
Delegated-IPv6-Prefix-Pool support	We have enhanced IPv6 prefix delegation by allowing the RADIUS server to specify a prefix pool name to cnBNG. The cnBNG uses this information to assign IPv6 prefixes to subscribers.
Tunnel-Preference support	You can now prioritize specific tunnels for data transmission when multiple tunnels are available. The Tunnel-Preference attribute in RADIUS messages allows you to specify the preferred tunnel, offering greater flexibility in tunnel selection.
Tunnel-Client-Auth-Id support	This attribute supports tunneling protocols by specifying the authentication name used by the tunnel inititator during the authentication phase of tunnel establishment.
PPPoE session limit based on circuit-id and remote-id	You can now limit the number of PPPoE sessions on a designated UP and PPPoE profile, using PPPoE Circuit-ID and Remote-ID as criteria. This feature ensures that when the session-limit is exceeded, cnBNG will reject new subscriber session requests associated with the specific Circuit-ID and Remote-ID.

Feature	Description
Automated standby-state recovery	This feature eliminates manual intervention by automatically transitioning CP-GR cluster instances from the "STANDBY_ERROR" state to "STANDBY" after a geo-replication switchover.
Handling L2TP Sessions during CP-GR switchover	This feature minimizes downtime and ensures smooth transitions during network changes by disconnecting existing L2TP sessions and tunnels during a CP-GR switchover. It then establishes new sessions on new tunnels.

Related Documentation

For a complete list of documentation available for this release, go to:

https://www.cisco.com/c/en/us/support/routers/cloud-native-broadband-network-gateway-bng/products-installation-and-configuration-guides-list.html

Installation and Upgrade Notes

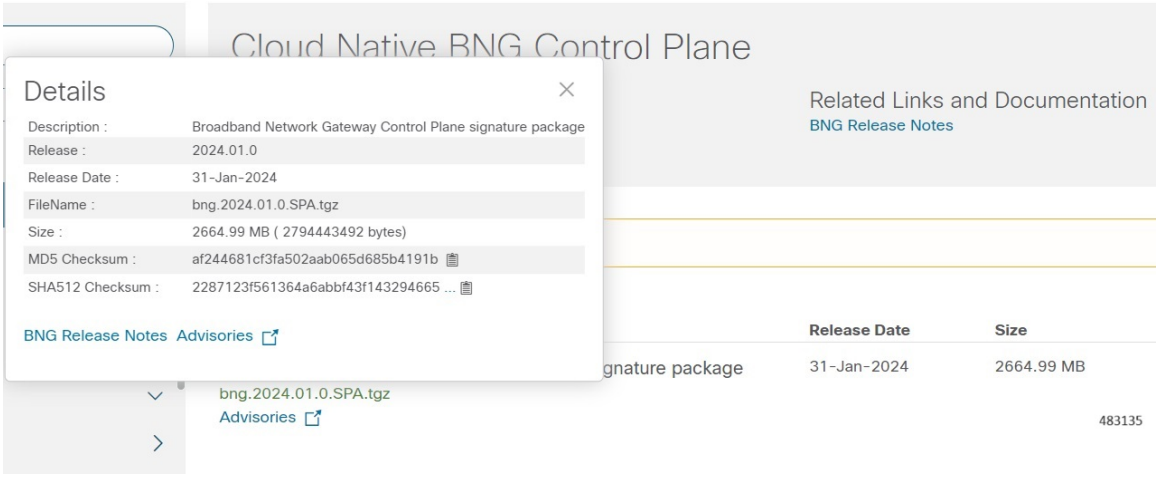
This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image you have downloaded.

The following screenshot is an example of a cnBNG CP release posted in the Software Download page.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, refer to the following table.

Table 1: Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command: **> certutil.exe -hashfile** *filename.extension* **SHA512**
Apple MAC	Open a terminal window and type the following command: **$ shasum -a 512** *filename.extension*
Linux	Open a terminal window and type the following command: **$ sha512sum** *filename.extension* Or **$ shasum -a 512** *filename.extension*
NOTES: *filename* is the name of the file. *extension* is the file extension (for example, .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

cnBNG CP software images are signed via x509 certificates. View the .README file packaged with the software for information and instructions on how to validate the certificates..

Open Bugs for this Release

The following table lists the open bugs in this specific software release.

Note This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

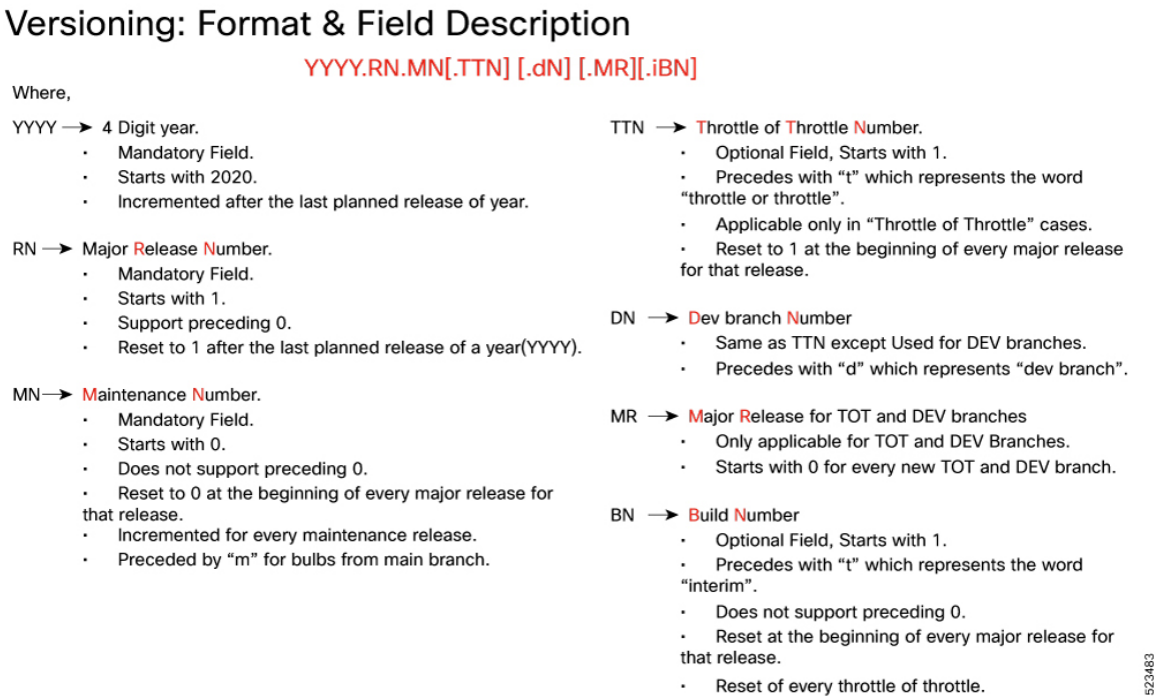
Bug ID	Headline
CSCwo90139	[SVI-April'25] Continuous n4-affinity errors

Bug ID	Headline
CSCwo54152	Evaluation of Cisco Ultra Cloud Core - SMI for Apache Tomcat RCE 2025 Vuln
CSCwp07620	udp-proxy pod restarted after adding of multiple VIP IPs under the end-point

Operator Notes

Cloud Native Product Version Numbering System

The show helm list command displays detailed information about the version of the cloud native product currently deployed.



The appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format facilitates identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

The following table provides descriptions for the packages that are available with this release.

Software Packages	Description
bng.<version>.SPA.tgz	The cnBNG CP offline release signature package. This package contains the cnBNG CP deployment software as well as the release signature, certificate, and verification information.
ncs-<nso_version>-bng-nc-<version>.tar.gz	The NETCONF NED package. This package includes all the yang files that are used for NF configuration. Note that NSO is used for the NED file creation.
ncs-<nso_version>-cisco-bng-smi-deployer-<version>.tar.gz	This is the NSO Core-Function-Pack for Day 0/Day 1 installation of cnBNG CP.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html.