Cisco Prime Network 4.3.2 Release Notes

Revised: February 19, 2019

This document contains the following sections:

- Introduction, page 2
- New Features and Enhancements, page 2
- Important Notes, page 4
- Prime Network 4.3.2 Bugs Using Bug Search Tool, page 6
- Open Bugs in Prime Network 4.3.2, page 6
- Resolved Bugs in Prime Network 4.3.2, page 7
- Bugs Resolved in Earlier Releases but Still Open in Prime Network 4.3.2, page 7
- Accessibility Features in Prime Network 4.3.2, page 7
- Obtaining Documentation and Submitting a Service Request, page 8

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco Prime Network 4.3.2 provides service providers and other network operators with a comprehensive assurance and device management solution for IP next-generation networks (NGNs), mobility, data center, and cloud. It is offered as a standalone application and as a fully integrated component of the Cisco Prime Carrier Management suite for customers needing end-to-end network management lifecycle capabilities. It provides standards-based interfaces to integrate with OSS applications.

The Cisco Prime Network 4.3.2 primarily supports the following features and enhancements:

- Security Hardening
- Path Tracer support on FEC129 Pseudowire
- Support for adding Element IPs to the database manually for Prime Central-Fault Management Resync
- Long Description option in systems and security event notification
- Platform: RedHat 6.8 support with latest RPMs
- Virtual context VRF for back-up and configuration
- Oracle Patch update
- Suppression of IPv6 false service alarms on Virtual Interfaces
- StarOS Alarm Clear Correlation and Alarm correlation granularity

Note Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 4.2, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.

New Features and Enhancements

The following topics describe the new features and enhancements introduced in Prime Network 4.3.2:

- Enhancements in Prime Network Vision, page 2
- Enhancements in Operations Report (Pentaho), page 3
- Installation and Upgrade, page 3
- Administration, page 4
- New Module Support for Devices, page 4

Enhancements in Prime Network Vision

The following enhancement is described in the *Cisco Prime Network 4.3.2 User Guide*:

Suppress False Service Alarms on Virtual Interface

Ability to suppress or unsuppress virtual interface related service alarms on Device series or VNE or in **Tickets** tab by using *Runregtool* commands.

StarOS Alarm Correlation on Asr5k Devices

Support for clear correlation alarms is addressed by the attribute-specific Alarms on ASR5K mobility device.

Virtual Context VRF for Back-up and Configuration

Ability to perform CCM configuration and image management operation for IOS-XR devices through Virtual Routing and Forwarding (VRF).

Path Tracer Support on FEC129 Pseudowire

For Layer 2 path information, Cisco PathTracer uses VC ID, AGI, SAII, TAII, and label switching information to trace the path from one tunnel interface to another.

Enhancements in Operations Report (Pentaho)

Operation Reports Data Backup

Improved DLP file backup process is supported for Operation reports.

Installation and Upgrade

The following installation and upgrade features and enhancements are described in the *Cisco Prime Network 4.3.2 Installation Guide*:

Platform: RedHat 6.8 support with latest RPMs

- Red Hat 6.8 64-bit Server Edition (English language) is supported in Prime Network 4.3.2. It can run in a virtual environment and is supported on VMware ESXi version 4.0 and 5.5.
- Install Prime Network GUI clients from thick and thin clients in a remote PC (Windows 10 OS).

Element IP in Tickets and Integration Changes

Ability to add managed elements to the database manually for Prime Central-Fault Management Resync.

Note For this Element IP in Prime Central-Fault Management Resync feature to be supported in setups, which are upgraded to Prime Network 4.3.2, a BQL needs to be executed. For more information about the steps see the *Prime Network 4.3.2 Installation Guide*.

Oracle Patch update

You need to install the Oracle Patch in Prime Network with Embedded Oracle 12c to authenticate several security vulnerabilities. Ensure that the following updates are performed in Prime Network:

- During Prime Network fresh Installation with Embedded Oracle 12c, the Oracle 12c July 2016 patch is installed automatically.
- During Prime Network upgrade from 4.2.0 onwards, a prompt to Install Oracle 12c July 2016 Patch is displayed. Click **Yes** to install the Oracle 12c July 2016 patch or click **No** to skip the Patch installation.
- During Prime Network upgrade from 4.0 and 4.1, follow the Oracle Upgrade steps mentioned in the Prime Network 4.3.2 Installation Guide

Administration

The following new enhancements are described in the *Cisco Prime Network 4.3.2 Administrator Guide*:

Security Hardening

Ability to disable Low and Medium strength ciphers using a single ***updateciphers.pl*** script for device communication and multiple applications.

Long Description option in system and security event notification

View the Long description of event information for a system or security event.

Sending Source Exact Location Details (ASR5k)

Ability to send the ASR5k related traps with the new location details.

New Device Support Information

No New Device support is provided in Prime Network 4.3.2.

New Module Support for Devices

Prime Network 4.3.2 introduces module support for devices in the device packages released during January DP1701, March DP1703 and May DP1705. Additional device support will be available in the next DP. For more information about the module support of devices download the *Cisco Prime Network 4.3.2 Supported Cisco VNEs—Addendum document* on the Prime Network download site on Cisco.com.

Important Notes

This section provides important information of which you should be aware before using Prime Network 4.3.2.

Installation and Upgrade

Before performing any fresh installation of High Availability (HA), ensure that any label used by any cluster service to name a distinct block device on any node in the cluster, must be unique across all block devices on the nodes of the cluster. You need to run the command on all nodes of the cluster, and cross check across all results before configuring local HA cluster because, a label used in a cluster service may not be reused by any block device with a different UUID which is listed by command 'blkid'.

Non-Starting of Compliance Engine

If the compliance engine does not start, follow the below steps:

- Before upgrading to 4.3.2.0, take the backup file **nccmDatabase.properties** that is located in PNHOME/utils/independent/compliance/resources/server/global/nccmDatabase.properties.
- After upgrading to 4.3.2.0, replace the backed up file **nccmDatabase.properties**.
- Perform cmctl restart.

UnConfigured VDC

- The Unconfigured VDC in the logical inventory shows configuration detail with empty data.
- Differentiation between Unconfigured VDC and suspended VDC in Prime Network is not available.

PN-IL Health Monitor

By default, the PN-IL health monitor is disabled.

CCM Environment Limitations

1. The XMP process requires 64-bit Java environment.
2. The number of Linux memory pages should be increased to 8718 to support CCM.

To increase the Linux memory page size, perform the following steps:

a. Login to the Linux server as a pnuser.

b. Increase the number of pages in the server by entering the following command:
sysctl -w vm.nr_hugepages=8718

c. View the changes by entering the following command:
cat /proc/meminfo | grep Huge

Limitations in Compliance Manager

1. In Compliance Audit, few system AAA service policies show incorrect audit violations. For more information, see CSCvm56361.
2. In Compliance Audit, few Fix CLI commands are applied twice. For more information, see CSCvm84162.

Workflow and Activation Replaced With Transaction Manager

Activation and workflow features have been replaced with Transaction Manager. These features are no longer available in Prime Network.

Configuration Audit Features Available Only upon Upgrade

The configuration audit feature in Change and Configuration Management is deprecated and is being replaced with Compliance Audit. When you upgrade to Prime Network Version 4.3.2, the system prompts you about the Configuration feature. Based on your input, the Configuration Audit feature is enabled or disabled.

Cable Technology - uBR10K Devices

For uBR10K devices, cable modeling for Upstream and Downstream channels and complete modeling for the MC20X20V and MC3GX60V line cards will be only supported from versions 12.2(33)SCG5 and higher.

Browser Limitations for Prime Network Web Components

In Firefox 24, users might not be able to connect to the Prime Network 4.3.2 web server to use features such as VCB, Network Discovery, and CCM, using Firefox 24 if the gateway IP address is a raw IPv6 address. This issue seen because of Firefox defect. To avoid this issue, log in to Prime Network 4.3.2 using a hostname instead of an IP address.

Automatic Restart After Gateway Reboot

Prime Network 4.3.2 will restart automatically whenever the gateway server is restarted. This behavior can be disabled (so that Prime Network 4.3.2 has to be manually started after a gateway restart). See the *Cisco Prime Network 4.3.2 Administrator Guide* for more information.

Auto-Discovery of Unsupported Modules

Auto-discovery of unsupported module types is done on a best effort basis and is based on standard information which is reported by the device as part of the ENTITY-MIB. Operators are advised to validate that the discovery was fully successful. If not, add support for the specific module type using the VCB.

SNMP Configuration

When VNE is configured to use SNMPv2 or SNMPv3 for discovery, SNMPv1 must also be enabled with the device.

Prime Network 4.3.2 Bugs Using Bug Search Tool

Use the Bug Search tool (BST) to get the latest information about Cisco Prime Network bugs. BST allows partners and customers to search for software bugs based on product, release, and keyword, and it aggregates key data such as bug details, product, and version.

Bug Search allows you to:

- Quickly scan bug content
- Configure e-mail notifications for updates on selected bugs
- Start or join community discussions about bugs
- Save your search criteria so you can use it later

When you open the Bug Search page, check the interactive tour to familiarize yourself with these and other Bug Search features.

Step 1 Log in to the Bug Search Tool.

a. Go to https://tools.cisco.com/bugsearch/.

b. At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 2 To search for bugs in the current release:

a. Enter **Prime Network 4.3.2** in the Search For field and hit Return. (Leave the Product, Software Type, Release, and Show Bugs fields empty.)

b. When the search results are displayed, use the filter and sort tools to find the types of bugs you are looking for. You can search for bugs by severity, by status, how recently they were modified, according to the number of support cases associated with them, and so forth.

If you know the bug ID, simply enter it in the Search For field and hit Return.

Open Bugs in Prime Network 4.3.2

Table 1 lists the open bug in Cisco Prime Network 4.3.2 release. Click the Bug ID to view the impact and workaround for the bug in the Bug Search Tool. Use this tool to track the status of the open bug.

Table 1 Open Bugs

Bug ID	Description
CSCve35977	Evaluation of ana for struts 1 cumulated vulnerabilities.

Resolved Bugs in Prime Network 4.3.2

You can find detailed information about all resolved bugs in Release 4.3.2. For more information, see Prime Network 4.3.2 Bugs Using Bug Search Tool, page 6.

This search uses the following parameters:

Table 2 Resolved Bugs

Field	Parameter
Product drop-down list	Choose Series/Model and enter Cisco Prime Network.
Releases drop-down list	Choose Affecting or Fixed in these Releases and enter 4.3.2.
Filter	Choose Fixed from the Status drop-down list.

Bugs Resolved in Earlier Releases but Still Open in Prime Network 4.3.2

The bugs listed in Table 3 were identified too late in the Prime Network 4.3.2 development cycle to be fixed for this release. The fixes for these bugs have been provided to customers running older versions of the product as needed and are scheduled for inclusion in the next release.

Table 3 Bugs Resolved in Earlier Releases but Still Open in Prime Network 4.3.2

Bug ID	Description
CSCve03446	Service alarms not cleared due to racing conditions in DIA expedite registrations
CSCve37308	Port description issues in routing entity of Nexus 7k device.
CSCve40131	Nexus VNE does not update port status after line card OIR.
CSCvf06061	Nexus VNE creates “Power Supply out' and 'Fan-tray out' for fake modules.
CSCvd80359	Link/Line down syslog alarms for BE sub-interface erroneously associated with line LAG DC.

Accessibility Features in Prime Network 4.3.2

The Prime Network 4.3.2 software does not provide accessibility features. All product documents are accessible except for images, graphics and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

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, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Accessibility Features in Prime Network 4.3.2" section.

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.

© 2017 Cisco Systems, Inc. All rights reserved. Printed in the USA on recycled paper containing 10% postconsumer waste.