



Cisco Prime Network 4.2 Release Notes

Revised: May 20, 2015

This release notes document provides an overview of the new features and enhancements in Cisco Prime Network 4.2 and highlights important issues you need to know before using this release. It lists open bugs and how to access information on Prime Network 4.2 bugs in Bug Search.

Contents

This document contains the following sections:

- [Introduction, page 2](#)
- [New Features and Enhancements, page 2](#)
- [Important Notes, page 7](#)
- [Prime Network 4.2 Bugs, page 8](#)
- [Related Documentation, page 21](#)
- [Accessibility Features in Prime Network 4.2, page 22](#)



Introduction

Cisco Prime Network 4.2 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.


Note

IP NGN has been renamed as Evolved Programmable Networks (EPN). Please keep this in mind when viewing the suite and application documentation for the next Cisco Prime Carrier Management release.


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 4.2:

- [New Technology Support in Prime Network 4.2, page 2](#)
- [Installation and Upgrade, page 6](#)
- [Prime Network Integration Layer, page 6](#)

New Technology Support in Prime Network 4.2

Prime Network 4.2 adds device-level inventory modeling and event generation for the technologies listed below. For information on which technologies are supported on which Cisco devices, see [Cisco Prime Network 4.2 Supported Cisco VNEs](#).

Carrier Ethernet

Ethernet Virtual Private Network (EVPN)

- Support for the following EVPN bridge types:
 - Provider Backbone Bridge-Ethernet Virtual Private Network (PBB-EVPN)
 - Bridge Domain (BD)
- Ability to locate and view the EVPN container properties under logical inventory:
 - EVPN bridge types
 - EVPN backbone MAC (B-MAC) address entries
 - Import and export route targets

Ethernet Segment

- The Ethernet segment is a site that is connected to one or more Provider Edge (PE) switches. The Ethernet segment can be a single device such as a customer edge or an entire network. The Ethernet segment in a network can be of the following types:
 - Single-homed device (SHD)
 - Multi-homed device (MHD)
 - Single-homed network (SHN)
 - Multi-homed network (MHN)
- Ability to locate and view the following Ethernet segment properties under logical inventory:
 - Type of primary and secondary customer service interfaces provided by the I-Bridge Backbone Edge Bridge (IB-BEB). The primary or secondary customer service interfaces can be any one of the following: Port based, S-tagged, or I-tagged interface.
 - Redundancy group entries.

PBB-EVPN

- Support for the PBB-EVPN solution that combines Ethernet Provider Backbone Bridging (PBB - IEEE 802.1ah) with Ethernet VPN, where provider edges (PEs) perform as PBB Backbone Edge Bridge (BEB). Two types of PBB-EVPN bridge supported:
 - I-Bridge—Interfaces with the customer edge. The PBB-EVPN customer bridge is an I-bridge.
 - B-bridge—Interfaces with the core network. The PBB-EVPN core bridge is a B-bridge.
- Ability to locate and view the following PBB-EVPN core bridge and customer bridge properties under logical inventory:
 - VSI information.
 - Unique route distinguisher per customer.
 - Multiple MAC Registration Protocol (MMRP).
 - Pseudowire, I-Bridge associations, and Ethernet flow point (EFP) information.

Provider Backbone Bridge (PBB)-Virtual Private LAN service (VPLS) (PBB-VPLS)

- The VPLS is a class of VPN that supports the connection of multiple sites in a single bridged domain over a managed MPLS network. The VPLS is a multipoint service and it can also transport non-IP traffic. A VPLS network consists of the following three main components—Customer edges, provider edges, and IP/MPLS core network.
- Two types of PBB-VPLS bridge supported:
 - I-Bridge—Interfaces with the customer edge. The PBB-VPLS customer bridge is an I-bridge.
 - B-bridge—Interfaces with the core network. The PBB-VPLS core bridge is a B-bridge.
- Ability to locate and view the following PBB-EVPN core bridge and customer bridge properties under logical inventory:
 - VSI information.
 - Unique route distinguisher per customer.
 - Multiple MAC Registration Protocol (MMRP) associations.
 - Pseudowire, VPLS I-Bridge associations information.

Provider Backbone Bridge (PBB)-Multiple MAC registration protocol (MMRP) (PBB-MMRP)

- MMRP operates on the services provided by the Multiple Registration Protocol (MRP). It allows bridges, switches or other similar devices to register or unregister attribute values such as VLAN identifiers and multicast the group membership information across a large LAN.
- Ability to locate and view the following PBB-MMRP core bridge and customer bridge properties under logical inventory:
 - MMRP participants.
 - MMRP registration properties and registered neighbors.

Support for Pseudowire FEC 129

- Single-segment pseudowires (SS-PWs) using FEC 129 on an MPLS PSN can use both type 1 and type 2 AII. For an MS-PW using FEC 129, a pseudowire itself is identified as a pair of endpoints.
- Ability to locate and view the following pseudowire end-to-end emulation tunnels properties under logical inventory:
 - New addition in pseudowire type as FEC129 TYPE II.
 - Source Access Individual Identifier (SAII) of the tunnel.
 - Target Attachment Individual Identifier (TAII) of the tunnel.

Support for Pseudowire Headend Layer 2 and Layer 3 sub interfaces

- The pseudowire headend (PW-HE) sub interfaces technology is supported from ASR 9000 device version 5.1.1.
- Provides Layer 3 termination of the access pseudowires into a Layer 3 Service PE (S-PE/N-PE) device such as ASR 9000 devices.
- The Layer 2 sub interfaces are attached to a bridge domain to forward packets whereas the Layer 3 sub interfaces have their own IP addresses and these interfaces are attached to a VRF.
- The path trace and flow are supported in the PW-HE interfaces. Before PN 4.2, any packet that is received from the Layer 2 pseudowire was redirected to Layer 3 IP interface of the PW-HE interface.

Satellite Network Virtualization (nV) Service Support

- The Cisco ASR 9000 Series Router Satellite Network Virtualization (nV) service or the Satellite Switching System enables you to configure a topology in which one or more satellite switches complement one or more Cisco ASR 9000 Series routers, to collectively realize a single virtual switching system. The Satellite nV system supports the dual-homed network architecture, based on which two hosts are connected to a satellite through the Satellite Discovery And Control (SDAC) Protocol.
- The advanced satellite nV system network topologies can be realized based on one of these architecture:
 - Hub and Spoke
 - Ring with Dual Home
 - Ring with Layer 2 Fabric
 - Linear and Cascade
- Locate and view the following satellite properties under logical inventory for the ASR 9000 Series routers.
 - Satellite connections and satellite fabric links details.

- Satellite ICCP group redundancy system properties that include control interfaces and access data link aggregations.

Mobility

Small Cell Solution

- Ability to optimize and monetize consumer and business services on mobile devices across 3G and 4G networks.
- Ability to locate and view the service details that includes IURH based Femto-to-Femto handoff and IURH handoff guard timer for Home Node B (HNB) gateway.
- Ability to locate and view crypto template for Home evolved Node B (HeNB) access gateway.
- Ability to locate and view the following service details for HeNB services gateway:
 - ANR info retrieval.
 - Public warning system.
 - Default paging DRX.
 - S1AP max retransmissions and timeout.
 - SCTP param template.
 - eNodeB Type.
 - Quality of Service (QoS) Differentiated Service Code Point (DSCP) used over the S1 MME service.
- Ability to locate and view the following service details for security gateway:
 - The peer list name for WSG service site-to-site mode.
 - Initiator and responder mode duration.
 - Enable duplicate session detection to allow only one IKESA per remote IKE-ID.
 - View Crypto map configuration information.
 - View IKE SA configuration and child IPSec SA configuration information.
 - View CA certificate configuration information.
 - View the connected applications configuration information.

SAMOG

- The SaMOG gateway service runs on a Cisco ASR 5000 chassis with the StarOS operating system. The SaMOG gateway provides seamless mobility between the 3GPP EPC network and WLANs for Evolved Packet System (EPS) services, functions as a 3GPP Trusted WLAN Access Gateway (TWAG) as the Convergence Gateway (CGW) service, and functions as a 3GPP Trusted WLAN AAA Proxy (TWAP) as the Multi Radio Management Entity (MRME) service.
- Ability to view configuration details for the following services of the SaMOG gateway under logical inventory—SaMOG service, CGW service, and MRME service.

Cisco Virtualized Packet Core (VPC)

- Cisco Virtualized Packet Core (VPC) provides single solution for all the packet core services (for 4G, 3G, 2G, Wi-Fi, and small cell networks). As the network functions are provided as virtualized services, VPC enables you to scale capacity and introduce new services in a faster and cost-effective manner.

- VPC is based on the same proven StarOS software used in Cisco ASR 5000 Series platforms.
- VPC is mainly designed to distribute and orchestrate packet core functions across physical and virtual resources to enable user to perform transition from physical to virtualized packet core services, or use both simultaneously.
- Support to view the Element type of the Virtual ASR 5K SI Mobile-Gateway either as Single instance (SI) or Distributed instance (DI).

Virtualized Service Module (VSM)

- Support of VSM card in any slot on the Cisco ASR 9000 Series Aggregation Services Router (ASR90xx and ASR99xx). The Cisco ASR 9000 VSM Card has the capability to run hypervisor on it. The hypervisor (example KVM) can host a single VM.
- Ability to locate and view VSM card with slot configuration details under physical inventory.
- Ability to view configuration details of KVM host server and virtual service gateway such as Wireless Security Gateway (WSG) under logical inventory.
- Support to view the virtual machines configured for KVM host server under datacenter option in logical inventory.

Installation and Upgrade

The following new installation and upgrade features and enhancements are described in the [Cisco Prime Network 4.2 Installation Guide](#):

- Enhanced GUI installation wizard that simplifies the installation experience and improves the speed of installation
- GUI installation wizard for Prime Network Integration Layer installation.
- Enhanced client download page with recommended installation for 32-bit and 64-bit operating systems.
- Support for Red Hat 5.8 and Red Hat 6.5.
- Embedded Oracle database upgraded to Oracle 12c.
- Support for VMware ESXi version 5.1 and 5.5.

Prime Network Integration Layer

Prime Network 4.2 introduces the following new integration layer features and enhancements:

- New GUI installation wizard for quicker and easier installation of the PN-IL. For details, see the [Cisco Prime Network 4.2 Installation Guide](#).
- MTOSI inventory support to retrieve a specific network function for small cell integration.
- Support for security gateway inventory retrieval in the Virtualized Service Module (VSM) card on the Cisco ASR 9000 Series Aggregation Services Router (ASR90xx and ASR99xx).

Important Notes

This section provides important information of which you should be aware before using Prime Network 4.2.

Installation and Upgrade

Operations Reports does not support IPv6. The gateway, database server (Oracle and Infobright), and the units should be installed with IPv4.

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 upon Upgrade Only

The configuration audit feature in Change and Configuration Management is deprecated and is being replaced with Compliance Audit. While upgrading from Prime Network 4.1 to 4.2, the upgrade procedure checks the user for configuration feature. Based on the user input, the Compliance Audit feature is enabled.

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, users might not be able to connect to the Prime Network 4.2 Web server to use features such as VCB, Network Discovery, and CCM using Firefox if the gateway IP address is a raw IPv6 address. This is due to a Firefox defect. To avoid this issue, log into Prime Network 4.2 using a hostname instead of an IP address.

Potential Image Management Issues on ASR 9000 Devices with very large configuration

Under some circumstances the device driver (VNE) representing an ASR 9000 device can enter and remain in a state that affects Prime Network 4.2's ability to display installed IOS-XR packages and distribute IOS-XR images to the device. While Prime Network 4.2 can continue to monitor the device and update the physical and logical inventory, the condition affecting the image management functionality will persist. This issue has been observed on occasion with densely populated ASR 9000 devices, and Cisco is working on resolving it. If you encounter this issue, try restarting the VNE.



Note

This issue is applicable to any device that is not in operational state.

Changing Command Builder when in Suite Mode

Command Builder access privileges can be controlled from the Prime Network 4.2 Administration GUI client, even when using Prime Network 4.2 in suite mode.

Automatic Restart After Gateway Reboot

Prime Network 4.2 will restart automatically whenever the gateway server is restarted. This behavior can be disabled (so that Prime Network 4.2 has to be manually started after a gateway restart). See the [Cisco Prime Network 4.2 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, ensure that the device must be enabled with SNMPv1 also.

Prime Network 4.2 Bugs

This section contains the following information:

- [Open Bugs, page 8](#)
- [Using the Bug Search Tool, page 21](#)

Open Bugs

The following sections identify bugs that are open in Prime Network 4.2, according to the following criteria:

- All catastrophic and severe bugs (if any).
- Customer-found bugs.
- Moderate, minor, and enhancement bugs that are considered likely to affect the customer's experience with Prime Network 4.2.
- Bugs that were fixed in previous releases of Prime Network 4.2 but are still open in the current release because they were identified too late in the Prime Network 4.2 development cycle.

The open bugs have been grouped in the following categories:

- [Installation/Upgrade Bugs, page 9](#)
- [High Availability Bugs, page 9](#)
- [Bugs Related to Hardware or Software Version Issues, page 9](#)
- [Technology-Related Bugs, page 10](#)
- [VCB Bugs, page 11](#)
- [Change and Configuration Management \(CCM\) Bugs, page 12](#)
- [Command Manager Bugs, page 12](#)
- [Fault Management Bugs, page 12](#)
- [Transaction Manager Bugs, page 13](#)
- [Report Manager Bugs, page 13](#)
- [Operations Reports Bugs, page 13](#)
- [VNE/AVM Bugs, page 14](#)
- [Suite-Related Bugs, page 15](#)
- [GUI-Related Bugs, page 15](#)

- [Job Scheduler Bugs, page 16](#)

Installation/Upgrade Bugs

Table 1 *Installation/Upgrade Bugs*

Bug ID	Description
CSCuq22556	Installing PN using GUI did not respond.
CSCuq52715	AVM 25 on UNIT is not able to connect to Oracle database due to missing JDBC information in the XML file "UNIT persistency.xml" while upgrading from Prime Network 3.11 to 4.x.
CSCuq63274	Installation fails in local HA when the name of a mount is available in the substring of another mount, for example mount names such as db and dbdata.
CSCun29698	The file auto_install_RH.ini contains passwords in clear text after installation.
CSCur73577	PN 4.2 Installations fails with timeout message due to OS prompt issue.
CSCur60321	Changing the PN gateway IP address displays error message.
CSCuq18115	Operation report installation fails in Local HA configuration.
CSCur44497	When configuring system using the capacity planning spreadsheets, the profile requirements are not clear, and leads to setup failing due to disk size errors.
CSCur59909	Errors in the AVM (AVM25) log file.
CSCut16609	Unable to upgrade from PN 4.1/4.0 with RHEL 6.4 to PN 4.2 with RHEL 6.5.

High Availability Bugs

Table 2 *High Availability Bugs*

Bug ID	Description
CSCun70782	PN-HA emdbctl script switches remote DB to read only.
CSCun39020	Missing remote mount folder fails cluster second node installation.
CSCuo99877	When nodes have different NIC names, PN installation fails.

Bugs Related to Hardware or Software Version Issues

These are hardware or software version specific issues that are causing bugs in Prime Network 4.2.

Table 3 *Bugs Related to Hardware or Software Version Issues*

Bug ID	Description
CSCuq49902	Due to SNMP flapping, VNE changes the state from operational to Currently unsynchronized state in Cat4500X-32 device.
CSCuq69723	RSP card name changes after OIR in ASR903 device.
CSCuq71718	When remote port value for satellite port is increased, then the new value is not updated.

Table 3 *Bugs Related to Hardware or Software Version Issues (continued)*

Bug ID	Description
CSCuq80772	Mismatch in physical inventory found in ME2600 device.
CSCur70468	Sup redundancy state is in NA after performing standby Sup instead of standby state. The reason being, the device sends the following syslog "%MODULE-5-STANDBY_SUP_OK: Supervisor 6 is standby", but PN fails to parse the syslog.

Technology-Related Bugs

Table 4 *Technology-Related Bugs*

Bug ID	Description
CSCun59446	STP blocking decoration is not displayed on a VLAN overlay, when there is more than one link between the devices.
CSCur65803	The path tracer does not include inner VLAN, when starting the path trace from Ether Flow Point in EVC (in the service view map).
CSCur79402	The interface status down alarms for RSP management interfaces and ICL IP interfaces are not cleared, after the chassis got connected to the ASR 9001 device.
CSCup91729	Changing the MAC address of a port automatically changes the bandwidth to 0 bps on Ethernet LAG.
CSCuq24225	Tunnel TP Interface status down does not correlate with Link down ticket.
CSCun85984	Incorrect tickets are generated while performing transceiver OIR in ASR 9000 device.
CSCun18551	When a VSI is removed and then rediscovered, it is represented by a reconciliation icon rather than as a new object.
CSCun47761	The EFP is not displayed on the pseudowire and EVC service views.
CSCuq70067	The OAM Admin status for any port in OAM Tab is not matching with that status of the port under Physical Inventory.
CSCuo86912	The EFD does not split after shutting down the link.
CSCuh95425	Network event does not show up for CPT RP switchover syslog.
CSCuh37319	Config syslog changes take a long time to update in the GUI for MPBGP in Nexus 7000 and Nexus 5000 devices.
CSCuh46377	Cross launch from Generic server port to PPM fails. This happens because Prime Network uses ifName from IF-MIB and normalizes the port name for better UI presentation.
CSCun00130	When reloading an ASR9K device, a "Port down due to Admin" ticket might be generated on a port that is already in admin down state.
CSCun27884	Alarm association location shows physical interface instead of VLAN, which is defined correctly in location OID.
CSCun19328	Some entries in the "EFPs" table contain extra data that does not exist anymore in the polled data or are missing data that exist in the polled data.

Table 4 **Technology-Related Bugs**

Bug ID	Description
CSCun08829	ASR 5000 VNE becomes unreachable every polling cycle for a period of around two minutes when there are a few thousand AAA Diameter Route entries.
CSCum70578	TP Tunnel is missing in the map pseudowire view.
CSCum54365	Prime Network stops discovering TP tunnel services. AVM35 process hangs, TP-tunnel Service Discovery plug-in stops working.
CSCun13956	Missing entries in Label Switching table and VRF Label table for ASR 9000 IOS XR 4.3.2.
CSCum95128	Missing pseudowire links and incorrect pseudowire overlay.
CSCun04198	Preferred path is not shown in the logical inventory for VSI-based pseudowires on ASR 9000 devices.
CSCug20371	When shutting down a multilink interface, the MLPPP link disappears instead of becoming red.
CSCum85797	Menu option "Get Virtual Connections" is disabled on E1 ports.
CSCtu27429	MPLS topology test is based on ip instead of LDP neighbors.
CSCum27966	Wrong network events correlation if management VRF name mismatches on different contexts (default and non-default) on Nexus nodes.
CSCuh56824	Deleting or stopping a large scale VCenter VNE takes a long time.
CSCuh43963	On a Cisco CRS S/W 4.3.0 modeled with "Reduced Polling", deleting IPv4 from an interface is not reflected in the inventory until the "POLL NOW" button is clicked on the card level.
CSCun33376	Service alarms are not generated when deleting a VSI from the device.
CSCun20899	Active and backup pseudowires did not merge.
CSCun13111	Pseudowire seems empty in the EVC view If both edges are of type Bridge/VSI.
CSCun16609	"Chassis temperature exceeds 65 degrees" trap which is not supported anymore is still listed in the client.

VCB Bugs

Table 5 **VCB Bugs**

Bug ID	Description
CSCuq90423	Adding a large number of VCB event patterns using CLI fails.
CSCur73782	While importing a large number of commands using VCB fails.
CSCur87477	The System default module templates available in Cisco Entity MIB Modules can be deleted after editing them.
CSCur87458	VCB is showing the wrong Overriding System Default status.
CSCur41822	Unable to remove or delete some user-defined items from the system.

Change and Configuration Management (CCM) Bugs

Table 6 *CCM Bugs*

Bug ID	Description
CSCuq42856	Restoring archive backups fail in overwrite mode in CCM for CPT600 device.
CSCun57035	CCM image backup does not work on a NAT environment.
CSCuq29047	Configuration restores on CCM fails for ASA 5585 device.
CSCun55948	The PN-NCCM fails for configuration operations through the SCP MWR294.
CSCum99969	When trying to activate 500 devices in one job the storage pane rendering is slow and it takes a long time to populate data.
CSCup85500	Image activation task for ASR 5500 device is successful in NCCM but showing timeout errors.
CSCuq42594	The second and subsequent configurations of CCM backup for CPT devices fail but Prime Network displays successful message.
CCSctq26336	When the Nexus 7000 VNE is stopped, its configuration archives are removed.
CSCug63646	After restoring archived config to startup-config on an ASR 903 device, the latest startup-config is not retrieved although the configuration is different.
CSCum09408	Restore job failed for ASR9000 device.

Command Manager Bugs

Table 7 *Command Manager Bugs*

Bug ID	Description
CSCun70765	Selecting 1000 devices in Compliance Audit using SHIFT+CLICK is not possible.
CSCun83339	The delete fails when a new implementation is added to an existing command.
CSCur66647	Command Builder script for ME1200 results in protocol failure.
CSCuo93145	CB display does not support command for CPT in CTC mode.

Fault Management Bugs

Table 8 *Fault Management Bugs*

Bug ID	Description
CSCuq17839	After modeling ASR 9000 devices with satellite, verify the link between two chassis discoveries and perform the card down operation. A ticket with "chassis disconnect" is created. While performing the card down and port down operations, similar tickets should be created.

Transaction Manager Bugs

Table 9 *Transaction Manager Bugs*

Bug ID	Description
CSCur49529	Devices are not listed for Device role as Configurator in Transaction Manager.

Report Manager Bugs

Table 10 *Report Manager Bugs*

Bug ID	Description
CSCur78886	Hardware summary report generated by selecting Properties displays empty report.

Operations Reports Bugs

This table shows open bugs in the new Prime Network Operations Reports component.

Table 11 *Operations Reports Bugs*

Bug ID	Description
CSCuh63290	No option to select an output type (HTML, PDF, etc.) when scheduling an interactive report.
CSCuh63304	When editing and then saving a prepackaged interactive report, the name of the report is changed.
CSCuh60084	Report scheduled with recurrence value of “run once” disappears from the Workspace after it has been executed.
CSCuh57022	Only the Prime Network user (pnuser) should be allowed to start/stop Operations Reports processes but the root user can also do this by running the reports server start/stop server script (./ctl.sh under export/home/<pnuser>/pentaho/server/biserver/tomcat/scripts).
CSCui14086	Data source was deleted and cannot be retrieved.
CSCui37467	Only the first page of a scheduled interactive report is shown although the report contains multiple pages.
CSCun00271	Interactive reports execution is slow with setups of more than 30K devices.
CSCun18255	Inventory data report stops responding and remains “in-progress” for a long time.
CSCug14300	Bottom scroll bar in interactive reports is not fully visible.
CSCug34500	Drop down list does not disappear when performing a subsequent action.
CSCug34580	Tooltip is not clearly visible in Operations Reports GUI.
CSCuh21737	In the Active Events interactive report, the text does not wrap and field values overlap into the next field.
CSCuh59716	For pre-packaged interactive report scheduling email option not provided.

Table 11 **Operations Reports Bugs (continued)**

Bug ID	Description
CSCuh60062	Scheduled interactive report names in Workspace not recognizable.
CSCuh60113	"Schedule" option is not enabled for pre-packaged reports.
CSCuh60722	Scheduled Interactive reports are all shown in the same page.
CSCus07901	When Prime Network is upgraded, the Operation Reports is not upgraded to latest version of Prime Network.

VNE/AVM Bugs

Table 12 **VNE/AVM Bugs**

Bug ID	Description
CSCuo97690	Missing contextual launch link in VM dashboard for Hypervisor name and server.
CSCup02954	SFP pluggable status is not refreshing while performing SFP input and output operations.
CSCun12892	The CLI state is UP, when VNE password is changed to incorrect value.
CSCun20740	The Nexus 7000 IPv6 routing table is not updated after poll now operation.
CSCum15296	There is no physical link shown between the ASA 5585 and 3560 devices.
CSCuq65696	In PN, the AVM crashes after making some operations on the device.
CSCur77350	Device proxy for Telnet session displays with incorrect prompt.
CSCup01703	NW discovery is not running after stopping existing discovery profile.
CSCuo80394	The Power supply out or in ticket is not correlated in a single ticket.
CSCui81411	Bridge table is not modeling in Nexus 1000 devices.
CSCum48310	Power supply syslogs and traps are not correlating to ticket for FEX module.
CSCur57576	The syslog parsing rule NODE-STATE-CHANGE-DOWN does not expedite card status registration.
CSCur17591	SNMP link down and link up traps are not processed correctly.
CSCuq99569	No change in sub interface status even when VRF is removed in the far-end of pseudowire.
CSCur45007	Number of MAC addresses in the bridge-domain 'BDN-NCN_ADMIN-00001' has reached the maximum configured MAC address limit. No notification is sent and syslog is not processed.
CSCum68808	When testing power supply unit failure on ASR 5500 devices, it was noticed that PowerFilterUnitUnavail (.1.3.6.1.4.1.8164.2.33) and PowerFilterUnitAvail (.1.3.6.1.4.1.8164.2.34) trap alarms are not associated with power supply units.
CSCuq93887	EFP operational state is not updating when the bridge is shutdown.
CSCuq96585	The VNE driver component is missing for ASR 902 Fan.
CSCur72204	Links are not discovered. Physical inventory displays missing interfaces and logical inventory in the CDP table does not show local interface.

Table 12 VNE/AVM Bugs (continued)

Bug ID	Description
CSCuq97343	Adding a new driver for Red Hat Linux sysoid in VCB is not making the VNE to discover it as Red Hat Linux but still as generic compute server.
CSCur16288	The 'Power Supply down' ticket opened when power cord was disconnected, has not been cleared when power cord was reconnected.
CSCur30027	The environmental trap events must have unique identifier.
CSCur36847	Port type for management ports of ASR5500 UMIO is displayed incorrectly.
CSCur36849	Management ports of ASR5500 UMIO displays no transceiver message.
CSCur68162	VNE modeled through SSH should act the same way when logged in through Telnet. CCM job fails when "Ask for user credentials when running device configuration operations" is not checked from the product GUI.
CSCur83400	VNE logs multiple Java exceptions such as NullPointerException, NumberFormatException, IllegalArgumentException and so on in various parts of the VNE driver code in ASR 5000 devices.
CSCur83563	IPv4 metrics at interface level in ISIS is showing incorrect metrics data.
CSCun43731	When the satellite chassis is disconnected, a duplicate "Power supply out" alarm is triggered that does not get cleared.
CSCun54905	Satellite ICL links do not show up for ASR9K device with XR 511.
CSCuq69330	Deadlock in AVM 11 while importing a script named VcbImportCommands.sh.
CSCur25505	AVM25 in the unit fails to connect to the database after several gateway failovers.

Suite-Related Bugs

Table 13 Suite-Related Bugs

Bug ID	Description
CSCuh93423	The Prime Central GUI may temporarily show Logical DC entities (VM, Host, Host Cluster, etc.) after a vCenter is deleted from Prime Network.
CSCut08164	Unable to perform cross launch from VNE to Prime Provisioning in a suite environment.
CSCut05315	Login to Operation report failed in a suite environment.

GUI-Related Bugs

Table 14 GUI-Related Bugs

Bug ID	Description
CSCur83592	IE 10 did not work with Prime Network 4.1 and 4.2 Application Launch pages with hostname in URL.

Job Scheduler Bugs

Table 15 *Job Scheduler Bugs*

Bug ID	Description
CSCun17110	In some cases, the Command Builder script returns different results when executed manually than when executed by means of a scheduled job.

Resolved Bugs

Table 16 identifies bugs that were listed as open bugs in the Prime Network 4.1 release notes and have since been resolved.

Table 16 *Resolved Bugs in Cisco Prime Network 4.2*

Bug ID	Description
CSCui05381	Device Proxy support for key based authentication requires users to change jar files.
CSCum94855	Tickets with sandglass are generated for missing notification <to check>.
CSCun79708	Notifications are not being sent.
CSCun95386	Compliance Audit Page at times renders with a "js" error.
CSCun95760	Compliance audit job fails while using the SCP protocol.
CSCuo04758	CCM fails to distribute image to Dragon wave devices while using the FTP facility.
CSCuo04951	Command Manager, administrator, and configurator is unable to view jobs of other users.
CSCuo14797	A leak in file descriptors, and the SSH socket is not destroyed on disconnect.
CSCuo22448	Special character in configuration fails the Config Audit job.
CSCuo34442	Compliance audit generates a wrong violation report.
CSCuo35057	Lotem does not gracefully close the SSH session at device response timeout.
CSCuo60826	The activate Cisco IOS by Image page does not render properly. This is observed in Internet Explorer 8 and above.
CSCuo70655	PN4.2 Local HA + Geo Installation fails.
CSCup00772	CCM configuration on ASR 5500 device is not restored even though the operation is successful.
CSCup12335	Administrator login page disappears after the login.
CSCup12483	Unable to login to Admin Client in the Local HA + Geo setup.
CSCup12636	Unable to launch web Admin Client in the Geo Only setup.
CSCup22047	Multiple issues in OpenSSL.
CSCup36688	Unable to launch web Admin Client after switchover on VM or BM in Geo Only.
CSCup44741	Catastrophic hot backup failure on Local HA + Geo only in a BM setup.
CSCup62864	Device IP selector instead of Unit IP in the VCB trap sender window.

Table 16 Resolved Bugs in Cisco Prime Network 4.2

Bug ID	Description
CSCup78313	Admin or configurator is not able to see other user's jobs.
CSCup81783	Unable to login to Admin client.
CSCup81839	Unable to launch Web Admin client.
CSCup89911	Slow response in AVM OOM and device due to multiple XML command instances.
CSCuq01417	Geo only installation failure in VM setup.
CSCuq09015	XMP is not installed properly when installing PN 4.2 gateway.
CSCuq30244	VCB syslogs are not processed in Prime Network due to space character.
CSCuq30874	Local HA + Geo installation failure in VM setup.
CSCuq30902	Geo only installation fails in VM setup.
CSCuq31390	Unit failover did not work for few work flows in PN.
CSCuq52320	Issues exist in setFpingPermissions.tcl when searching for PN home directory.
CSCuq57439	Issue in anactl and/or cmctl for compliance on unit.
CSCuq60886	nvSatellite ICL links slow discovery issue in Topology link.
CSCuq72556	User scope in CCM operation does not work.
CSCuq93458	CCM upgrade issues while performing an upgrade on PN4.2.
CSCuq94869	upgrade.pl fails on permissions update.
CSCur05741	Local HA installation fails in VM setup.
CSCur08897	Telnet collector gets stuck at Lotem (jcraft) and hence the VNE is in an unsync mode.
CSCur32612	Catastrophic hot backup fails on Local HA + Geo only.
CSCur32629	Non-Catastrophic hot backup fails on Local HA + Geo Setup in a VM environment.
CSCur40812	AVM 25 exception caused by: java.lang.ArrayIndexOutOfBoundsException
CSCur43466	Embedded Oracle upgrade issues when performing an upgrade from PN 11 to PN.
CSCur48627	Add commands filter does not select the right commands.
CSCur49474	PN 4.2 GUI installation searches for Oracle 11G.
CSCur53183	Command Manager is extremely slow while creating a new command.
CSCur67937	Non-Catastrophic Hot backup fails on Local HA + Geo setup,
CSCur76129	Modeling issues for CPT device inventory in PN 4.2
CSCug85781	Duplicate BFD connectivity down service alarms displayed on LAG interfaces.
CSCui33244	Administrator GUI fields for LDAP DN prefix and suffix are too short.
CSCui88402	Logger total counter returns a negative number.
CSCuj75462	MLPPP medium priority member down event is not created when the T1 controller is down.
CSCul08868	BFD syslog events are not correlated with BFD services events.
CSCul61005	Hardware detailed report for ports displays wrong PID data.
CSCum15154	Tickets created for LAG interfaces down are not cleared.
CSCum82990	Duplicate memory usage registrations exist for Cisco ASR 5500 VNE.

Table 16 **Resolved Bugs in Cisco Prime Network 4.2**

Bug ID	Description
CSCun19151	Satellite IC port status does not have status populated on VNE.
CSCun24906	Fan tray out ticket is not cleared and fan status is displayed as cleaning in PN.
CSCun68861	The source MAC address column in the Y1731 probe table is empty for Cisco ASR9000 and 9904 series devices.
CSCun82767	Source MEP column is empty in ASR9000 and 9904 devices.
CSCun84997	ReportsServiceImpl is null for RegistryManager.
CSCuo17407	IRD framework in waiting state is not responding.
CSCuo68860	BfdSessionCommandHandler is added twice to the waiting list and causes OOM.
CSCuo85863	Inconsistent reporting of DWDM controller state as AdminDown or Down.
CSCup00169	While removing an RSP card, chassis disconnect alarm is generated.
CSCup75674	Delayed false service alarms for pseudowire links.
CSCup78077	EFP polling registration should be changed to Bypass Compare.
CSCuq21235	Change XML registration should be persistent with optimized command.
CSCuq36948	Link is not reflected between Cisco ASR 9000 device and WSG service in Prime Network.
CSCuq46566	Pentaho initialization exception on PN 4.2.
CSCuq56260	Multiple IndexOutOfBoundsException is displayed in CiscoRouterIOXREMrouteParser.
CSCuq60823	Forge VSM syslogs are not reflected in Prime Network.
CSCuq61701	Tags such as rttMonCtrlAdminTag must be added as distinguisher for IPSLA trap events.
CSCuq65175	Empty table is populated for MMRP participants in I-Bridge.
CSCuq67351	Contexts are not getting modeled.
CSCuq74630	PN does not send virtual flag as false for VPC in unavailable state.
CSCuq80527	In Cisco ASR 5000 devices, all services are not modeled under the context.
CSCuq85912	Get Inventory for host server full information displays exception.
CSCuq93527	Bean shell error exists while executing SNMP command in Prime Network.
CSCuq97306	Cisco ASR 5000 packet services cards are not properly discovered.
CSCur02125	Notifications are not sent when adding, editing, or deleting H(e)NB, MME, HNB, GSN, and service gateways.
CSCur16167	Memory usage is not displayed in device inventory of ASR 5500 devices.
CSCur16391	Traps such as starHNBGWWSGSNRanapReset, starHNBGWMSRanapReset are treated as standard traps.
CSCur31759	ISIS Implementation and modeling to be changed for Cisco IOS XR devices.
CSCur36333	OAM parser fails to return empty IRD list when no OAM is configured in Cisco ASR 9000 devices.
CSCur44628	The TE tunnel properties parser (CiscoRouterCRSMplsTETunnelPropertiesParser) fails to parse the TE path option.

Table 16 *Resolved Bugs in Cisco Prime Network 4.2*

Bug ID	Description
CSCur45016	MAC address limit trap is not parsed.
CSCur46296	SFP 1000BASE-T cards are not discovered properly.
CSCur48201	The EVPN and bridge container in PN is not updated on removal of EVPN.
CSCur54704	Physical inventory is not modeled correctly for Cisco ASR 5000 device in PN 4.0.
CSCun10969	650K message are dropped every 30 seconds.

Closed Bugs

Table 17 identifies bugs that have been closed since the previous release.

Table 17 *Closed Bugs in Cisco Prime Network 4.1*

Bug ID	Description
CSCuh68380	Reports folders are not visible when Operations Reports is launched for the first time.
CSCuf48387	Pie chart distribution is not equal to 100% in report.

Bugs Resolved in Earlier Releases but Still Open in Prime Network 4.2

The bugs listed in [Table 18](#) were identified too late in the Prime Network 4.2 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 18 *Bugs Resolved in Earlier Releases but Still Open in Prime Network 4.2*

Bug ID	Description
CSCu198786	When CDP is disabled, an expectation for the topology to be discovered through MAC topology is established, and links are not discovered.
CSCum54365	TP tunnel service discovery plugin stops working and AVM35 process continues without stopping.
CSCun19143	Satellite IC port status participating in ICLs does not have status populated on initial investigation of VNE.
CSCun92962	Select devices screen in USCC results in blank execution parameter screen from IE 8.
CSCun37851	Issue in event “IntegritySP.creTicketOrArchiveFlaggingEvent” displays database exception.
CSCuo02196	CDP link between Cisco 2811 (Serial0/0/0.111) and ASR 1000 (Serial0/1/0.1/1/1/1:0.111) devices is missing.
CSCun24955	In UPC telecom test setup, PW to TP stitch is missing periodically in PW service at Network Pseudowire and Pseudowire Edge levels.
CSCuo19812	ASR 9000 device performs modeling for a long period of time and this causes 50% CPU usage on the unit. Empty table is populated for MMRP participants in I-Bridge.
CSCup21269	Collector agent is suspended when a command script is executed.
CSCup21205	Events that are not stable creates proxy events for traps.
CSCun37125	Fault DB does not have the PPM TCA trap recorded.
CSCun90467	The Layer1 or Layer2 topology links between T1 interfaces with PPP and MLPPP configuration are not discovered in Prime Network 3.11.
CSCup65479	When bandwidth on the bundle Ethernet interface is configured to be lower than maximum speed of combined members' port speed, then the Ethernet channel inventory continue showing a maximum value.
CSCup87393	Audio alarm gets broken if the ticket gets cleared quickly.
CSCun95767	Saving a command fails for ASR 1001 device series.
CSCuq02423	When using FTP as a transfer protocol, CCM fails to backup configurations from Dragonwave devices.
CSCuq07357	Binding information is not available on EFP.
CSCur02707	Telnet command in Network Vision needs to use the protocol set in the VNE.
CSCur75222	In CRS8S platform, the fan-tray out ticket is not created when the fan tray is removed.
CSCui35119	Configuration restore operation fails.
CSCuj28308	CIOS image version is UNKNOWN in the Repository window.

Using the Bug Search Tool

Bug Search is a new tool for getting information about Prime Network 4.2 bugs. In addition to having better performance than the legacy Bug Toolkit, 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** Access the Bug Search tool from the Bug Toolkit page.
- a. Go to <http://tools.cisco.com/Support/BugToolKit>.
 - b. At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.



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** Open the Bug Search page by clicking the **Bug Search** link from the top of the Bug Toolkit page.
- Step 3** To search for bugs in the current release:
- a. Enter **Prime Network 4.2** 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.

Related Documentation

For a list of the guides available for Prime Network 4.2, see the [Cisco Prime Network 4.2 Documentation Overview](#).

Additional information can be found in the Cisco Prime Network Technology Center, which is an online resource for Prime Network support content, including help for integration developers who use Prime Network application programming interfaces (APIs). It also provides a platform for you to interact with subject matter experts. To access the Prime Network Technology Center website, you must have a Cisco.com account with partner level access, or you must be a Prime Network licensee. You can access the Prime Network Technology Center at: <http://developer.cisco.com/web/prime-network/home>.

Accessibility Features in Prime Network 4.2

The Prime Network 4.2 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 “[Related Documentation](#)” 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.

© 2014 Cisco Systems, Inc. All rights reserved. ♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.