Cisco Prime Network 3.10 Release Notes

Revised: February 28, 2013

This release notes document provides an overview of the new features and enhancements in this release, highlights important issues you need to know before using this release, and describes how to access information on Prime Network 3.10 bugs.

Note You can access the most current Prime Network documentation, including these release notes, online at http://www.cisco.com/en/US/products/ps11879/tsd_products_support_series_home.html.

Contents

These release notes contain the following sections:

New and Changed Information

The following table describes information that has been added or changed since this document was first published.

Date Released	Revision	Location
February 28, 2013	CCM Device Support—Added that a complete list of devices that support CCM in this version of Prime Network is provided in the *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.10*.	Change and Configuration Management, page 7 New Device Support Information, page 11
November 2012	Initial release.	—

Introduction

Cisco Prime Network 3.10 provides service providers and other network operators with a comprehensive assurance and device management solution for IP next-generation networks (NGNs). It is offered as a standalone application and as a fully integrated component of the Cisco Prime IP NGN suite for customers needing end-to-end network management lifecycle capabilities.

Until now, Prime Network's operations support functionality has been focused on the network traffic transport and distribution areas of service provider networks. In this release, Prime Network expands its device operation and administration and network assurance support to:

- Wire line subscriber network infrastructures: BNG
- Mobility: LTE support
- Datacenter infrastructures: UCS, Nexus, datacenter connectivity and virtualization
- Network Virtualization (nV): ASR 9000 cluster and satellite

Important Notes

This section provides important information of which you should be aware before using Prime Network 3.10.

Automatic Restart After Gateway Reboot

Prime Network 3.10 will automatically restart whenever the gateway server is restarted. This behavior can be disabled (so that Prime Network has to be manually started after a gateway restart). See the *Cisco Prime Network 3.10 Administrator Guide* for more information.

Auto-Discovery of Unsupported Modules

In Prime Network 3.10, a new mechanism to automatically discover unsupported module types was introduced. The discovery 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.

StarOS 14.0 - Disabled MIBs

Starting from StarOS 14.0, the following MIBs are disabled by default in the device.

- ENTITY-MIB

- F-MIB

- ENTITY-STATE-MIB

- CISCO-ENTITY-FRU-CONTROL-MIB

The physical inventory will not be modeled if these MIBs are disabled. Enable the MIBs using the following:

```
configure
snmp mib ENTITY-MIB
snmp mib IF-MIB
snmp mib ENTITY-STATE-MIB
snmp mib CISCO-ENTITY-FRU-CONTROL-MIB
```

To verify if the above MIBs are enabled, use:

```
show snmp server
```

New Features and Enhancements in Prime Network 3.10

The following topics describe the new features and enhancements introduced in Prime Network 3.10:

- New Technology Support in Prime Network 3.10, page 3

- Additional Device Configuration Scripts, page 5

- Prime Network Administration, page 6

- Change and Configuration Management, page 7

- Fault Management, page 8

- Command Builder, page 9

- Job Management, page 9

- Reports, page 9

- VNE Customization Builder (VCB), page 9

- Prime Network Integration Layer, page 9

New Technology Support in Prime Network 3.10

Prime Network 3.10 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 3.10 Supported Cisco VNEs*.

Carrier Ethernet

- Y.1731 IPSLA probes

- In topology views showing Ethernet Virtual Connection(s), Prime Network 3.10 allows the addition of a CPE network element to the map and manual attachment of the device to an edge Ethernet Flow Point (EFP).

MPLS-TP

- MPLS-TP bulk lockout—Allows locking or unlocking multiple MPLS-TP tunnels on different VNEs at the same time. This is required when performing maintenance in the network. It enables you to divert the MPLS-TP packets through an alternative LSP.

Multicast

Prime Network 3.10 provides the first phase of support for multicast, focusing on representation of multicast configuration attributes and monitoring of events.

- IP Multicast - representation of baseline IPv4 and IPv6 configurations
- MPLS Multicast - representation of multicast Label Distribution Protocol (mLDP) and multicast VPN (mVPN) configuration attributes for IPv4 and IPv6 on PE routers

Satellite and Cluster Technologies

- ASR 9000 cluster support:
  - Chassis inventory shown in physical inventory
  - Table showing all physical ports connecting the Active and Backup Chassis in the cluster
  - Support for cluster-related traps and syslogs
  - Inter-chassis link state shown in inventory
- Topology visualization for multi-chassis devices—ASR 9000 host device plus satellites are represented in the map as an aggregation that can be expanded. When the aggregation is expanded, the host and satellite devices are represented separately with inter-chassis links.

Broadband Network Gateway (BNG)

- BNG policies and global configuration attributes discovered and shown in logical inventory
- IP pool management and monitoring
- Retail model of BNG with PPPoE PTA and IPoE subscriber support
- Required AAA, Radius Server components & attributes
- DHCP (IPv4) profiles for IP subscriber
- BBA groups for PPPoE subscriber
- Dynamic templates for IP & PPP subscriber
- Class of Service (Class-Map)
- QoS and Subscriber control policies

Mobility

Prime Network 3.10 completes the second phase of support for LTE gateway functionality by representing:

- GGSN service configurations on ASR 5000 and ASR 5500 devices.
- StarOS APN service configurations
- StarOS P-GW and S-GW service configurations
- GPRS Tunnel Protocol Prime (GTPP) accounting configurations on ASR 5000 and ASR 5500 devices.
- Operator policies, APN remaps, and APN profiles
- StarOS configurations for Evolved GPRS Tunneling Protocol Control (EGPTC) messaging

- AAA configurations including AAA groups and diameter endpoints

- IP address pool configurations and association to service contexts on ASR 5000 and ASR 5500 devices

- System Architecture Evolution (SAE) Gateway configurations on StarOS that combine S-GW and P-GW functionality

- Local time zone of ASR 5000 and ASR 5500 devices

- ACS configurations

- PCRF faults generated by CPM 3.0 installed over UCS

Data Center

- Covers aggregation layer support (VDCs on Nexus), compute support from UCS physical inventory to the virtualization layer (hosts and VMs)

- Compute virtualization:

  - Inventory collection and visualization of the physical/virtual environment, limited to auto-discovery of hypervisors and VMs and compute resources, i.e., CPU and memory.

  - Mapping of the hierarchical relationships between virtualized components - servers and virtual machines.

  - Representation of the relationship between UCS blades, hypervisors and VMs

- Representation of FabricPath configuration attributes on Nexus 5000 and 7000 devices

- Representation of configuration attributes for the Virtual Port Channel feature on Nexus 7000 and Nexus 5000 series devices

Redundancy Modeling

Enhanced modeling of redundancy and representation of redundancy parameters in the physical inventory.

Additional Device Configuration Scripts

Prime Network 3.10 provides new predefined configuration scripts to configure the following services on ASR 5000 and ASR 5500 devices:

- GGSN, APN, GGTP, GTPU, EGTP, and DHCP

- P-GW and S-GW

- Home Agent, Subscriber, HA SPI List, AAA Group, Route Map, Route Access List, and Proxy DNS Intercept List

- Active Charging, RuleDef, RuleBase, AccessRuleDef and GroupOfRuleDef

- Port Interface, BGP, VRF, and BFD

Prime Network Administration

The following new features and enhancements are described in the *Cisco Prime Network 3.10 Administrator Guide.*

Session and User Management

- New Session Manager GUI which tracks all active GUI and NBI user sessions. Session Manager can be used to disconnect sessions and request users to re-login, or completely terminate sessions.

- New configurable global account inactivity period which, when exceeded, disables a user's account. The account can be re-enabled from the Administration GUI client.

- New configurable global password rules:

  - Configurable popup message that reminds users that their password is about to expire.

  - Configurable setting to control how many consecutive characters from a previous password *cannot* be used.

- New per-user authorization mode for job scheduling in global security settings. When this mode is enabled, individual users can be granted permissions to schedule jobs across the product. Users who do not have job scheduling permissions will not be allowed to schedule jobs.

> **Note** See also Command Scripts and Activations, page 7, for information on other configurable options you can use to manage how users run command scripts and activations.

Script to Change Gateway IP Address

New script for updating the Prime Network registry with a new gateway IP address.

Embedded Database

The **embdctl** command provides a new option that changes the SMTP server for e-mail notifications from an embedded database

Adaptive Polling

New Adaptive Polling tab in the VNE properties dialog box for fine-tuning adaptive polling (how Prime Network responds when a device has a CPU spike). After setting the upper and lower CPU thresholds, the following can be configured:

- The number of polls required to move a VNE from normal polling to slow polling, and from slow polling to maintenance mode (where all polling except for CPU usage is suspended)

- The number of polls required to move a VNE back to regular polling

- The delay (in milliseconds) between SNMP and Telnet commands that are sent from the VNE to the device.

Reduced Polling (Event-Based Polling) for VNEs

Reduced polling is now the default polling method for all VNEs and is also supported by the Network Discovery mechanism. This default setting can be changed, if necessary. If a VNE does not support reduced polling, it uses regular polling.

If desired, you can "force" reduced polling for a VNE. In this case, if the VNE does not support reduced polling, Prime Network will generate a Device Unsupported event. This is controlled from the Polling tab in the VNE properties dialog box.

Event Notification Service

The Event Notification Service has been enhanced as follows:

- Notifications can include network element properties (such as an interface description) and business tags in order to provide more information about the alarm source

- Notifications can include the alarm location as a user-friendly string (instead of an Object Identifier)

- Multiple notification services can use the same destination IP and port (UDP only). For example, you can forward these two services to the same destination:

    - One notification service that forwards specific service events for a group of VNEs

    - Another notification service that forwards syslogs and traps for a different group of VNEs

Command Scripts and Activations

- Configurable option to require users to enter their device access credentials when executing an activation or command script (as opposed to using the Telnet or SSH credentials defined for the VNE). The device user name is listed in Provisioning and Audit events, allowing you to track user actions. For cases in which this option is not supported (scheduled commands or activations or for SNMP commands), the VNE's Telnet or SSH credentials will be used.

- Configurable option to display a message upon execution of commands or activations, warning the user that the action might interrupt services. The system provides a default message which can be edited in the Commands and Activations global settings. In addition, when creating a command script using Command Builder, the message can be edited or the global setting can be overridden.

VNE-Specific Features

- Support for changing a VNE IP address without having to create a new VNE.

- Support for networks where two VNEs have the same IP address.

- Ability to configure global defaults for VNEs:

    - SNMP V1/V2 community read/write credentials and SNMP V3 authentication and encryption settings (new VNEs use SNMP V2 by default)

    - Telnet and SSH V1/V2 credentials

- VNE schemes:

    - New EMS scheme which only polls devices for system information and physical inventory

    - Ability to create customized schemes so you can specify which technologies and topologies you want Prime Network to model and monitor

- Support for TL1 parameters in the VNE creation editor (for using Configuration and Change Management on Cisco Carrier Packet Transport devices)

- Enhanced **ivne** script with a new option to display only the most recent VNE Device Package that is installed on the gateway (rather than simply listing all installed packages)

Change and Configuration Management

The following new Change and Configuration Management features and enhancements are described in the *Cisco Prime Network 3.10 User Guide.*

- Configuration Audit—the ability to audit configurations on a device against a specified baseline configuration policy file. The configuration policy is compared with the actual running configuration on the device, discrepancies are identified and published in a report.

- Scheduling of configuration and image management jobs is limited to users who have permissions to perform the operation.

- For configuration and image transfers, the TFTP directory available in the Prime Network gateway and/or unit can be modified using commands.

- For Cisco Carrier Packet Transport (CPT) devices, the Prime Network unit user credentials must be added to the registry. This is required because Prime Network initiates the FTP operation using a TL1 interface, and the TL1 commands require the username and password as input parameters. After you add this information to the registry, the credentials are automatically read when needed.

- Flash Player version 10 or higher must be available to view the Configuration Restore page.

- Configuration Restore—For Cisco CPT devices, the Running option restores the selected configuration to startup config and then to running config on the device.

- While importing images from an external repository or from a file system, CCM displays all images or packages (bin, pie, smu, and so on) from the directory specified in the Image Management Settings page, and also from its sub directory, in order to support tar files.

- Ability to perform an in-service software upgrade (ISSU) for Cisco ASR 903 devices and Cisco Carrier Routing System (CRS) to update the router software with minimal service interruption.

- Ability to modify boot priorities for Cisco ASR 5000 series devices and then perform activation.

- Satellite support for Cisco ASR 9000 devices, as follows:

  - Synchronization of all satellites together without activation.

  - Activation of the satellite pie image on Cisco ASR 9000 device with and without synchronization of satellites. You must run a CLI/XML command to check for compatibility and then push the image to the remote satellite.

For a complete list of devices that support CCM in this version of Prime Network, see the *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.10*.

Fault Management

The following new fault management features and enhancements are described in the *Cisco Prime Network 3.10 User Guide.*

- Stronger alignment with ITU-T Recommendation X.733 by displaying fault nature (ADAC or ADMC) and category (communications, QoS, processing, and so on).

- Provision of probable cause and recommended action for ASR 5000 traps to aid in troubleshooting fault conditions.

- Integration of traps from Cisco Prime Performance Manager (PPM) version 1.3—The Prime Network Event Collector receives threshold crossing alarm (TCA) events from PPM components and generates tickets that can be viewed in Prime Network Events.

- Event and ticket properties show the date and time when the ticket was created, based on the time zone of the device (For ASR 5000 and ASR 5500 devices)

- New (predefined) Events Troubleshooting Info report that provides probable cause and troubleshooting information for traps

- Several Event Notification Service enhancements. See Prime Network Administration, page 6.

Command Builder

- When creating a command script, a new Text Area input type is now available. This enables cutting and pasting multi-line strings, including end of line characters <CR><LF>. This is referenced in the script as a single attribute.

- User-authentication based execution of activations or command scripts (if this option is enabled in Prime Network Administration).

- Warning of potential service interruption upon execution of commands or activations (if this option is enabled in Prime Network Administration). The message can be edited or the global setting can be overridden when creating a command script.

Job Management

- Ability to clone a job and then edit the job properties. For example, after scheduling a command to run on certain devices, you can clone the job and then add/change devices.

Reports

The following new reports are provided in Prime Network 3.10 and described in the *Cisco Prime Network 3.10 User Guide.*

- Database Monitoring—Shows the state of the database at regular time intervals (e.g., hourly), over a specified period of time. Examples of information shown in this report are number of active tickets, alarms, events, biggest ticket ID, actionable event rate per second, and so on.

- Events Troubleshooting Info—Shows probable cause, action to be taken, and the clearing condition for events.

VNE Customization Builder (VCB)

Several enhancements have been made to the VCB GUI for enabling support for unsupported traps. These enhancements are described in the *Cisco Prime Network 3.10 Customization Guide.*

- The VCB now allows bulk upload of MIBs.

- When defining subtype mapping, possible values for subtypes are displayed. Users no longer need to enter subtype values in a text field.

- Support can now be added for multiple traps in a single flow; the MIB does not need to be loaded again for each trap.

- Usability enhancements to the wizard for adding support for traps.

Prime Network Integration Layer

Prime Network Integration Layer allows Prime Network to seamlessly integrate with an OSS by leveraging standardized interfaces. This integration layer functionality can be conceived as an additional layer running on top of Prime Network exposing 3GPP and MTOSI web services. Furthermore, a migration from this standalone deployment to Prime Suite mode is possible, if a Suite environment is available. See the *Cisco Prime Central Quick Start Guide* for more information.

In this specific release, inventory management functionality has been provided, both over 3GPP and MTOSI. While the 3GPP inventory management functionality is for ASR5500 and ASR5000 device types capturing both logical and physical inventory data in 3GPP prescribed XML format, the MTOSI interfaces available in this release retrieve physical inventory data for devices supported by Prime Network. For details on the various operations supported in this release, please refer to the *Cisco Prime OSS Integration Guide for MTOSI and 3GPP*.

For information about setting up the integration layer in Prime Network, see the *Cisco Prime Network 3.10 Installation Guide*.

User Documentation Enhancements

The following user documentation changes have been made in Prime Network 3.10:

- The *Cisco Prime Network 3.10 Gateway High Availability Guide* is a new document that consolidates all of the information related to installing and managing gateway high availability using Red Hat Cluster Suite (RHCS) and Oracle Active Data Guard (ADG). All Red Hat HA-related information that was previously documented in the installation guide, has been moved to this guide. For information on gateway high availability using Veritas, please contact your Cisco representative.

- The *Cisco Prime Network 3.10 User Guide* now includes information on Change and Configuration Management (CCM), rather than having that information in a separate guide. In addition, descriptions of the command scripts that are packaged with Cisco Prime Network have been moved to the appropriate chapters of this guide and are no longer documented in the reference guide.

- The *Cisco Prime Network 3.10 Administrator Guide* has been reorganized so that information related to the task you want to perform is easier to find. It also contains a new setup chapter that guides you through the initial tasks you should perform after installing Prime Network.

- The *Cisco Prime Network 3.10 Customization Guide* has been reorganized so that information related to the task you want to perform is easier to find.

- The *Cisco Prime Network 3.10 Installation Guide* has been reorganized to make it easier to follow the installation prerequisites and flow. The installation guide now describes Small, Medium, Large, and VM profiles with typical hardware combinations and event rates for Gateway and Unit. It also includes a chapter describing the next steps required after installation of Prime Network.

- The original Cisco Prime Network Reference Guide has been split into individual documents listing supported events, alarms, traps, syslogs, and technologies/topologies, as follows:

    - *Cisco Prime Network 3.10 Supported Cisco VNEs*

    - *Cisco Prime Network 3.10 Supported Service Alarms*

    - *Cisco Prime Network 3.10 Supported Security and System Events*

    - *Cisco Prime Network 3.10 Supported Syslogs*

    - *Cisco Prime Network 3.10 Supported Traps*

    - *Cisco Prime Network 3.10 Supported Technologies and Topologies*

New Device Support Information

Note Prime Network 3.9 with Device Package (DP) **1210** or later: After upgrading to Prime Network 3.10, you must install the latest DP from Cisco.com in order to have the same level of device support that you had in your earlier installation. This is because Prime Network 3.10 includes all of the support that is provided up to Prime Network 3.8.x-3.9.x-DP**1209**.

Prime Network 3.10 incorporates all the device support additions that were provided in Prime Network 3.8.x-3.9.x-DP1209 (the DP that was released in September 2012). To get the latest VNE support, please download and install the latest Prime Network DP from the Prime Network download site on Cisco.com.

For detailed information about new device support in Prime Network 3.10, please see *Cisco Prime Network 3.10 Supported Cisco VNEs*.

For a complete list of devices that support CCM in this version of Prime Network, see the *Addendum: Additional VNE Driver Support for Cisco Prime Network 3.10*.

Prime Network 3.10 Bugs

This section contains the following information:

- Open Bugs in Prime Network 3.10, page 11
- Resolved Bugs, page 17
- Closed Bugs, page 18
- Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.10, page 18

Open Bugs in Prime Network 3.10

The following sections identify bugs that are open in Prime Network 3.10, 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.
- Bugs that were fixed in previous releases of Prime Network but are still open in the current release because they were identified too late in the Prime Network 3.8.1 development cycle.

The open bugs have been grouped in the following categories:

- Installation/Upgrade Bugs, page 12
- Device and Software Version Specific Bugs, page 12
- Network Discovery Bugs, page 13
- Technology-Related Bugs, page 13
- VCB Bugs, page 15
- Change and Configuration Management (CCM) Bugs, page 15

Installation/Upgrade Bugs

Table 1   Installation/Upgrade Bugs

Identifier	Symptom
CSCud01686	New unit added after upgrade is in unreachable state.
CSCuc90531	Backing up Prime Network during upgrade fails with the following error: ./local/scripts/embedded_oracle/gen_database_files_to_remove.sql: Cannot open: Permission denied
CSCuc53525	Cannot log into the Prime Network GUI client after an upgrade from 3.8 to 3.10 in a Local HA setup,

Device and Software Version Specific Bugs

Table 2   Device-Related Bugs

Identifier	Symptom
CSCtw29586	FlashDevice Size is not modeled on Cisco ME3600 series device running Cisco IOS versions 15.1.2.EY and 15.1.2.EY1.
CSCtw65605	VEM module status shown as Unknown for Nexus 1000V.
CSCua33760	Oper states of back plane and fabric ports do not update properly after disconnecting the connection from chassis to IOcard.
CSCub55176	Card down/UP ticket is not raised for module N7K-F248XP-25 in EVNE for Nexus 7000
CSCub86764	IPv6 access list entries not modeled in ASR 9K,CRS and GSR XR devices.
CSCuc43901	Memory Usage graph is not updated for ASR 5000 and ASR 5500 devices.
CSCuc71849	On 7600 routers running IOS 15.1, multiple NullPointerExceptions are received in OspfInterfacePHLoader class and correspondingly, multiple OSPF property holders are not created.
CSCuc73922	When the ASR 9000 is configured with Clock and SyncE details, SyncE properties are shown as Unknown.
CSCuc90543	Nexus port admin status modeling incorrect for Nx-OS 6.1(1).
CSCuc92336	Power and Fan Rack, Modules are displayed without PID in the Prime Network Vision.
CSCub30191	Inconsistent or incorrect MAC Address modeling for Nexus VNE.
CSCty74187	ASR 5500 device, fan tray down service alarm is not cleared.
CSCty79971	ASR 5000 and ASR5500: When Virtual APN is deleted, it is still shown under main APN where it was referenced earlier

Table 2   Device-Related Bugs (continued)

Identifier	Symptom
CSCtq36525	Wrong PID shown for transceiver/SFP modules for Nexus 7000 device
CSCtu24056	CPU usage attribute is not populated in the GUI for SCE2000
CSCtw65605	VEM module status shown as Unknown for Nexus1000V
CSCud14121	Port up/down alarms are not generated for ports when Nexus 3000 is added using Reduced Polling.
CSCuc75229	For UCS device, some of the HBA and NIC Ports are not shown in the inventory.
CSCud18484	Chassis disconnected alarm will be raised in Prime Network when Nexus 2K is disconnected from Nexus 5K. However, it is not cleared when the connection is re-established in the device setup.

Network Discovery Bugs

Table 3   Network Discovery Bugs

Identifier	Symptom
CSCuc96102	When trying to create VNEs from devices discovered using Network Discovery, the VNEs are not created and the discovery result shows the devices in "Deleted" state after refresh. In this case, the devices are discovered with SNMP V3 with authentication but no encryption password.

Technology-Related Bugs

Table 4   Technology-Related Bugs

Identifier	Symptom
CSCuc39142	Out interfaces of TE Tunnels missing when one of the tunnel edge devices is reloaded.
CSCuc44069	Satellite IC port status participating in ICLs does not have status populated on initial investigation of VNE. Satellite ICL Link is not seen in the map.
CSCuc50104	Individual tickets are received for the same root cause, instead of showing as a single ticket with correlation
CSCuc76082	CFM MEP configured on Ether channel is not modeled and not shown in the logical inventory under the CFM container.
CSCuc77359	Clock PTP Service logical inventory is not populated on ASR 903 device. The clock PTP service logical inventory has a wrong PTP State for ASR901 device if the state on the device is either "Phased_Aligned" or "Freq_Locked".
CSCuc85097	Under Diameter Endpoints, Route health status displays invalid data for deleted or stale diameter peer.
CSCuc85479	AlarmStatusChangedEvent wrongly correlated to VMPower off and Power on Event in UCS Virtualization
CSCuc85484	Diameter peer with IPv6 address is not updated in Prime Network.

Table 4   *Technology-Related Bugs (continued)*

Identifier	Symptom
CSCuc91568	OSPF neighbor down service and ticket not created after the neighbor has been removed on ASR 903 device.
CSCuc92314	IPv6 Routing Table tab does not exists under ME3800 Routing Entity container in PN.
CSCuc97852	DWDM technology related properties show wrong/blank values under Physical Inventory for the ports under supported DWDM modules.
CSCtz80712	No alarm on a static link when its end is down
CSCtj30236	LAG link is not rediscovered after clearing and removing the ticket
CSCtu27429	MPLS topology test is based on ip instead of LDP neighbors
CSCuc54022	After initiation of 7609 device software upgrade, the VNE created 'BFD connectivity down' alarm which stays uncleared indefinitely although BFD session status was restored back to UP.
CSCuc74616	After IOS upgrade and router reload, the 7600 VNE was automatically restarted, dropping current state and disconnecting all the links. After the device and links were rediscovered, the OSPF Neighbor Down alarm correlated to corresponding Link Down root cause alarm was not cleared, keeping the resulting link alarm in Major state. Following Poll Now and VNE restart operation could not clear the alarm although inventory shows that the OSPF neighbor is UP.
CSCuc94395	ASR 9000: One of the remote peers' state shows up in the device inventory as blank when the neighbor's BGP state is 'Closing.'
CSCud09522	After a satellite chassis is disconnected and then reconnected, the ticket is not cleared and the satellite chassis is shown as OUT in Physical Inventory.
CSCub55128	LAG Down ticket is not raised when Port Channel is shut in Nexus 7K.
CSCud22188	Hosts that are part of one Datacenter are shown under a different Datacenter.
CSCud05474	Poll now is not working for following technologies on Nexus 7000 device: MPBGP, STP, Arp Table, Routing Table, Bridges, Ethernet LinkAggregation.
CSCud07691	VRF Routing Table is not modeling for Nexus 7K.
CSCud14557	Hosts that are part of one Data center are shown under a different Data center.
CSCud22188	Prime Network does not capture events for existing hosts after a new host is added to VCenter.
CSCub31023	When using the Integration Layer, inventory data related to APN DHCP always appears as empty although it might be actually configured in the device.

VCB Bugs

Table 5   Soft Properties Bugs

Identifier	Symptom
CSCtu33115	When adding support for third-party line cards that support multiple port types, port layers are not displayed correctly.
CSCud09747	"Failed to save data" error is thrown when trying to edit user-defined software versions
CSCuc81714	When adding traps from MIB, clicking the Analyze button in the upload dependencies step returns the same list that shows that the dependencies are not uploaded, and the process is stopped.
CSCuc13194	When committing a new syslog or trap through VCB, after pressing the Finish button, the application reports an error "Failed to save data: Timeout waiting for result".

Change and Configuration Management (CCM) Bugs

Table 6   CCM Bugs

Identifier	Symptom
CSCud09395	Copy startup-config to running-config will not work for CPT devices
CSCuc80341	When using theIE8 browser, a script error appears when clicking on the last run results page.
CSCuc80344	CCM sync page shows the "old" out of sync entry of the VNEs on IE8.
CSCuc52800	Job Schedule setting page does not show all years in the pulldown list of 'Start on date', it only shows a few years (1912-1918).
CSCuc06110	Sort order issue in Archived Configurations page in Change and Configuration Management.
CSCud15961	CCM does not launch when right clicking on a device in the map in Prime Network Vision GUI and clicking on Config Mgmnt or Image Mgmnt menu item.
CSCuc63379	Backup/restore running config job is not implemented.
CSCuc81181	Image upgrade does not work for ME3600x/ME3800X.
CSCud15947	Sync entry is not removed from sync page after performing synchronize job for IPv6 VNE.

Fault Management Bugs

Table 7   *Fault Management Bugs*

Identifier	Symptom
CSCtx01472	Newly added event types are not forwarded through the Event Notification Service if specific event types were selected when defining the service.
CSCuc67095	Event Notification Service does not forwarding business tag information on physical port.
CSCuc82018	In the Prime Network Administration GUI client, it is not possible to edit an existing Event Notification service that was created manually and that had registered for ticket severity updates.

Workflow-Related Bugs

Table 8   *Workflow-Related Bugs*

Identifier	Symptom
CSCud16596	Workflow execution failed, with "IllegalArgumentException: Invalid command syntax. no such command" error

Prime Network Vision/Events GUI Bugs

Table 9   *Prime Network Vision Bugs*

Identifier	Symptom
CSCuc71283	Cannot save map as PDF or SVG type.
CSCuc92247	Prime Network Events—When switching a tab and cancelling a running query, the next queries do not return results
CSCud05936	Existing value is not shown when renaming a service added to a map

VNE/AVM Bugs

Table 10   *VNE/AVM Bugs*

Identifier	Symptom
CSCuc81740	CPU goes up to 100% for a limited amount of time, then drops back to normal level.
CSCtj92252	For ISR 1800 device, VNE restarts due to software version change
CSCud12790	Adaptive polling mechanism incorrectly putting CRS into slow polling & maintenance mode. It never returns to normal even the usage is below low threshold for consecutive # polls defined in low_tolerance.
CSCuc86976	False CARD OUT alarms are received from ASR1006 and ASR 9006 devices
CSCuc96770	AVM crashes.

Table 10   VNE/AVM Bugs (continued)

Identifier	Symptom
CSCuc82722	Multiple VNEs with the same agentIDs in the avmxxx.xml files within the system.
CSCud05482	High load average may be caused because of southbound IP search.

Resolved Bugs

Table 11 identifies bugs that were listed as open bugs in the Prime Network 3.9 release notes and have since been resolved.

Table 11   Resolved Bugs in Cisco Prime Network 3.10

Identifier	Symptom
CSCua06195	When installing using GUI Unit is wrongly added as 0.0.0.1 in Prime Network GW
CSCua01831	ivne installer fails at the end of ANA 3.7.3 to Prime Network 3.9 upgrade
CSCtz71592	Migration: Error while upgrading from 3.8.1 to 3.9 with a unit behind NAT
CSCua18258	Switchover fails in a DR setup
CSCua31425	After upgrading to 3.9, downloading the client exe file fails and an HTTP 404 message is received.
CSCua39097	Unable to choose ipv6 address as the main ip interface when installing Prime Network on a full duplex unit.
CSCub43548	After uninstalling a GEO-HA environment, it was found that the Prime Network processes are still running in memory.
CSCts79008	Memory usage information is missing in Nexus 5000 device
CSCtw77988	ASR 9000 device: Missing bundle interface under Ethernet link aggregation in logical inventory
CSCtz80758	Unable to add vne with comma (",") in the telnet sequence
CSCtx67922	Inconsistent behavior of the appearance of NetworkTPTunnels under EVC
CSCtr35459	Cannot create Command Builder on subinterface 03.7(03.01)PP00,03.7(02.01)PP01
CSCtx29563	IPSec tunnels do not have tunnel status
CSCtz23017	IPSec tunnel does not show IP address when using unnumbered option
CSCts39840	BGP Neighbor Loss syslog is not correlated to Device Unreachable ticket
CSCtk65010	Wrong serial connection through CDP in MLPPP technology
CSCtz80426	MPLS TP End Points are not attached to Pseudowire Edges in service view
CSCtz70997	MplsTETunnel linkdown on the mid point or tail does not correlate to the headend if the headend is an ASR 9000 device
CSCua00802	Missing STP link
CSCtx39154	Adding a command builder script to Logical Inventory sub-menus remains in running state

Table 11 Resolved Bugs in Cisco Prime Network 3.10 (continued)

Identifier	Symptom
CSCua08248	Prime Network Change and Configuration Management uses the southbound IP of the unit server for file transfer between gateway and unit
CSCtr98822	ASR 5000 device: InterfaceTable-Input access list, Output access list+desc are blank
CSCty19414	TE-Tunnel down of IOS-XR devices do not correlate to Link-Down
CSCtz99804	ASR5000 and ASR5500: VRF interface under sites does not get updated on poll now
CSCua10049	ASR 5500: VRF interface is not reflected in Prime Network
CSCua19364	ASR1K: POS channels and POS interfaces on CHOC12 card are not modeled
CSCtz62728	cevGsrSIP601 card showing incorrect status in Network Vision physical inventory
CSCua33524	UCS-Nexus adjacencies are not showing in Prime Network
CSCua08070	Spelling/grammar errors in webcontrol script
CSCua24951	AVM becomes unreachable in a large CE setup

Closed Bugs

Table 12 identifies bugs that were listed as open bugs in the Prime Network 3.9 Release Notes and have since been closed.

Table 12 Closed Bugs in Cisco Prime Network 3.10

Identifier	Symptom
CSCtz86380	Port down alarm not cleared even though network event is resolved.
CSCua05419	Error in GUI reported "A data synchronization problem has been detected"
CSCth36256	Cisco Prime Network generates two separate link down events when a port is disconnected and connected a few times
CSCtz63105	Invalid 'Link down due to oper down' ticket
CSCth01054	Cisco 3750g fiber optic ports are modeled as RJ45 ports

Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.10

The bugs listed in Table 13 were identified too late in the Prime Network 3.10 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.

T

Table 13 Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.10

Identifier	Symptom
CSCtz41239	Incorrect outgoing interface for end-point LSPs on IOX devices
CSCua35492	'Chassis Connected' clearing service alarm will not appear when satellite chassis is reconnected for Multi-Chassis devices

Table 13   Bugs Resolved in Earlier Releases but Still Open in Prime Network 3.10 (continued)

Identifier	Symptom
CSCty91863	Mistake in checkPatchInstallation error message
CSCua59577	Device goes out of sync

Using the Bug Toolkit

This section explains how to use the Bug Toolkit to search for a specific bug or to search for all bugs in a release.

Step 1 Go to http://tools.cisco.com/Support/BugToolKit.

Step 2 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 3 To search for a specific bug, click the **Search Bugs** tab, enter the bug ID in the Search for Bug ID field, and click **Go**.

Step 4 To search for bugs in the current release, click the **Search Bugs** tab and specify the following criteria:

- Select Product Category—**Network Management and Automation**.

- Select Product—*Cisco Abstract Network Abstraction*.

> ✎
>
> **Note**   *Cisco Prime Network* is the new product name for the former *Cisco Abstract Network Abstraction*. At this time, the Bug Toolkit does not accept *Cisco Prime Network* as the product name.

- Software Version—3.10**.**

- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.

- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, click **Use custom settings for severity, status, and others** and specify the following information:

  - Severity—Choose the severity level.

  - Status—Choose **Terminated**, **Open**, or **Fixed**.

    Choose **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate suboption (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.

    Choose **Open** to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate suboptions that appear below the Open check box. For example, if you want to view only new bugs in Prime Optical 9.5, choose only **New**.

    Choose **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the Fixed check box and select the appropriate suboption (Resolved or Verified) that appears below the Fixed check box.

- Advanced—Check the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.

- Modified Date—Choose this option to filter bugs based on the date when the bugs were last modified.

- Results Displayed Per Page—Specify the number of bugs to display per page.

Step 5 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

✎

Note In the search results, the headlines and release-note enclosures might contain both *Cisco Prime Network* and *Cisco Active Network Abstraction* product names.

Step 6 To export the results to a spreadsheet:

a. In the Search Bugs tab, click **Export All to Spreadsheet**.

b. Specify the filename and location at which to save the spreadsheet.

c. Click **Save**. All bugs retrieved by the search are exported.

If you cannot export the spreadsheet, log into the Technical Support website at http://www.cisco.com/cisco/web/support/index.html or contact the Cisco Technical Assistance Center (TAC).

Related Documentation

For a list of the guides available for Cisco Prime Network 3.10, see the *Cisco Prime Network 3.10 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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.