Release Notes for Cisco Prime Infrastructure, Release 1.2

Last Updated: August 29, 2012
OL-27652-01

These release notes contain the following sections:

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

Introduction

The Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure provides two different graphical user interfaces (from which you can switch back and forth by clicking the downward arrow next to your login name):

- Lifecycle view, which is organized according to home, design, deploy, operate, report and administer menus.
- Classic view, which closely corresponds to the graphical user interface in Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).

For more information on the Lifecycle view of the Cisco Prime Infrastructure features, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/user/guide/prime_infra_ug.html

For more information on the Classic view of the Cisco Prime Infrastructure features, see the following URL:

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/configuration/guide/pi_12_cg.html

For more information on prerequisites, system requirements, and installation, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/quickstart/guide/cpi_qsg.html

Virtual Appliance - Hardware Requirements

Table 1 lists the hardware requirements for the virtual appliance based on wired/wireless scale. For information about the number and type of devices supported by each virtual appliance size, see the Cisco Prime Infrastructure 1.2 data sheet at http://www.cisco.com/en/US/products/ps12239/products_data_sheets_list.html.

Table 1 Virtual Appliance—Hardware Requirements

	Processor	DRAM	Hard Disk
Small Virtual Appliance	4 vCPUs	8 GB	200 GB
Medium Virtual Appliance	4 vCPUs	12 GB	300 GB
Large Virtual Appliance	16 vCPUs	16 GB	400 GB
Extra large Virtual Appliance	16 vCPUs	24 GB	1200 GB

Browser Support

Prime Infrastructure supports the following browsers:

- Google Chrome—19.0 build
- Mozilla Firefox— ESR 10.x, 13.0 and 14.0

- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in. Native Internet Explorer is not supported.

Note We recommend a minimum screen resolution of 1280 x 800 pixels.

Supported Software Versions

Table 2 lists the wireless devices and their software versions that are supported by Prime Infrastructure 1.2.

Table 2 Supported Controller Hardware Models and Software Versions

Controller Hardware Models	Controller Software Versions
Cisco 2100 Series	7.0.x
Cisco 2500 Series	7.0 and later versions
Cisco 4400 Series	7.0.x
Cisco 5500 Series	6.0 and later versions
Cisco Flex 7500 Series	7.0 and later versions
Cisco Flex 8500 Series	7.3
Cisco Virtual Controller	7.3
Cisco WiSM	7.0.x
Cisco WiSM2	7.0 and later versions
Cisco Wireless Controller on Service Ready Engine (WLCM2 on SRE)	7.2.110.0
Cisco Catalyst 3750G Series Integrated Wireless LAN Controllers	7.0 and later versions

For a complete list of supported WLCs and detailed information on the software compatibility for the Cisco wireless devices, see the following URL:

http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html

For detailed information on the supported device types and software versions, see the following URL:

http://www.cisco.com/en/US/products/ps12239/products_device_support_tables_list.html

Installation Guidelines

For detailed information about the installation guidelines, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/quickstart/guide/cpi_qsg.html#wp56681

Upgrading Cisco Prime Infrastructure

Note

- Install a patch to the existing system before performing the upgrade.
- Ensure that you perform a backup before attempting to upgrade.
- Use a console connection when you upgrade, to avoid Telnet/SSH terminal timeouts.
- Remove high availability before performing the upgrade.

The following are the NCS versions that you can upgrade from or backup/restore to Prime Infrastructure Release 1.2.0.103.

- NCS 1.0.2.29
- NCS 1.1.0.58
- NCS 1.1.1.24
- NCS/PA-WAN 1.1 (1.1.0.1114)
- NCS-WAN/PA 1.1.1 (1.1.0.1116)
- NCS 1.2.0.70 (Beta release)

For detailed information about the application upgrade, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/quickstart/guide/cpi_qsg.html#wp56675

Prime Infrastructure Feedback Tool

There is an automated feedback tool that can be configured to send periodic information to Cisco about the features that are being used on a given server. The feedback tool feature is disabled by default. You must enable this feature to identify the most frequently used features in Prime Infrastructure. You must configure the e-mail server and then enable data collection to configure the feedback tool.

To configure the feedback tool, follow these steps:

Step 1 Choose **Administration > System Settings > Mail Server Configuration**.

Step 2 In the Mail Server Configuration page, enter the mail server details.

Step 3 Click **Save** to save the configuration settings.

Step 4 Choose **Help > Help Us Improve Cisco Products**.

Step 5 In the Help Us Improve Cisco Products page, select the **Yes, collect data periodically** option.

Step 6 Click **OK**.

Submitting Feedback

To obtain support assistance and deliver feedback, use the following link to communicate with the Cisco support team:

https://www.ciscofeedback.vovici.com/se.ashx?s=6A5348A76B189D9B

Prime Infrastructure License

For detailed information on the Prime Infrastructure Licensing, see the following URL:

http://www.cisco.com/en/US/products/ps12239/products_data_sheets_list.html

Cisco Prime Infrastructure 1.2 Supported Devices

For detailed information on the supported device types, see the following URL:

http://www.cisco.com/en/US/products/ps12239/products_device_support_tables_list.html

New Features and Enhancements

The following topics describe new features and enhancements in Cisco Prime Infrastructure 1.2:

- Lifecycle Management, page 6
- The Virtual Wireless Controller, page 6

Lifecycle Management

The Cisco Prime Infrastructure supports lifecycle management of all your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure provides two different graphical user interfaces (from which you can switch back and forth by clicking the downward arrow next to your login name):

- Lifecycle view, which is organized according to home, design, deploy, operate, report and administration menus.
- Classic view, which closely corresponds to the graphical user interface in Cisco Prime Network Control System (NCS) or Cisco Wireless Control System (WCS).

The Virtual Wireless Controller

The virtual wireless LAN controller is a software that can run on hardware that is compliant with an industry standard virtualization infrastructure. Virtual wireless LAN controllers provide flexibility for users to select the hardware based on their requirement.

We recommend that you have the following hardware to host a virtual controller:

- Cisco UCS R210-2121605W Rack Mount Server (2 RU)
- IBM x3550 M3 server
- ISR G2 Services Ready Engine (SRE) using UCS Express

Cisco 8500 Series Controllers

Cisco 8500 Series Controllers are introduced with support for local mode, FlexConnect, and mesh modes. The Cisco 8500 Series Controllers support 6000 APs, 64,000 clients, 2000 FlexConnect groups, 6000 AP groups, 100 APs per FlexConnect group, and up to 4094 dynamic VLANs. A Cisco 8500 Series Controller can support up to 24,000 rogue APs and 32,000 rogue clients.

Increased Scale for Cisco Flex 7500 Series Controllers

Increased scale for Cisco Flex 7500 Series Controllers to support 6000 APs, 64000 clients, 2000 FlexConnect groups, 6000 AP groups, 100 APs per FlexConnect group, and up to 4094 dynamic VLANs.

Next Generation Maps

In addition to the features of the legacy maps, Cisco Prime Infrastructure 1.2 enables you to use the features of the Next Generation Maps. The Next Generation Maps feature is enabled by default. Use the **Administration > User Preferences** page to disable or enable this feature.

The Next Generation Maps feature provides you the following benefits:

- Displays large amount of information on map. When you have numerous clients, interferers and access points, these may clutter the display on Prime Infrastructure map pages. Also, pages load slowly. Prime Infrastructure 1.2 introduces clustering and layering of information. Information clustering reduces clutter at the high level and reveals more information when you click an object.
- Simplifies and accelerates the process of adding APs to the map. In the legacy maps, the process of adding access points to maps is manual and tedious. With Prime Infrastructure 1.2, you can use automated hierarchy creation to add and name access points.
- Provides high-quality map images with easy navigation and zoom/pan controls. In the legacy maps, the map image quality is low and navigating, zooming, and panning is slow. With Prime Infrastructure 1.2, you can use the next-generation ‘tile-aware’ map engine to load maps faster and zoom/pan easily. Also, Next Generation Maps enables administrators to load high-resolution maps faster and navigate around the map.

Automatic Hierarchy to Create Maps

Automatic Hierarchy Creation is a way for you to quickly create maps and assign access points to maps in Prime Infrastructure. You can use Automatic Hierarchy Creation to create maps once you have added wireless LAN controllers to Prime Infrastructure and named your access points. Also, you can use it after adding access points to your network to assign access points to maps in Prime Infrastructure.

FlexConnect-related Features

- Split tunneling allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic and the rest of the traffic as centrally switched.

  This feature is supported on the AP1040, AP1140, AP1260, AP3500, and AP3600 access points.

- Support to configure Network Address Translation (NAT) and Port Address Translation (PAT) on FlexConnect locally switched WLANs is added. You must enable Central DHCP Processing to enable NAT and PAT.

  This feature is supported on the AP1040, AP1140, AP1260, AP3500, and AP3600 access points.
- This release extends support for 802.11u in FlexConnect mode.
- 802.11r Fast Transition is now supported on FlexConnect APs in central and locally switched WLANs.
- VLAN-based local and central switching is supported. The AAA server returns a VLAN configured for a client. If the VLAN is configured on the local IEEE 802.1Q link, the AP bridges the traffic locally. If the VLAN is not configured on the AP uplink, the AP tunnels the traffic back to the controller. The controller bridges the traffic into the corresponding VLAN from where the traffic is transported toward the next routing instance for further processing.

HotSpot 2.0

This release extends support for HotSpot 2.0 specifications, where APs in mesh mode and APs in FlexConnect mode in locally switched WLANs are also supported.

Auto-Switch Port Tracing

This feature provides the ability to automatically identify the Cisco switch and port information for a rogue AP connected to the Cisco switch, which allows quickly identifying and mitigating the threat posed by a rogue AP.

Third Party Support

Ability to discover and monitor third-party (non-Cisco) switches that support RFC 1213 and wireless controllers/access points from Aruba Networks.

Proxy Mobile IPv6

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node, initiate the mobility signaling, and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Note PMIPv6 MAG functionality is supported only on Cisco 5500 series controllers, Cisco 8500 series controllers, and Cisco WiSM2.

VLAN Tagging

VLAN tagging on Ethernet interfaces is supported. You can configure VLAN tagging on the Ethernet interface either directly from the AP console or through the controller and Cisco Prime Infrastructure. You must save the configuration in flash, and all CAPWAP packets should use the VLAN tag as configured along with all the locally switched traffic, which is not mapped to a VLAN. When enabled, the CAPWAP packets from the AP are forwarded through the trunk VLAN. If it fails, the AP falls back to the untagged mode.

Support for New Access Points

This release introduces two new AP1552 models:

- AP1552CU
- AP1552EU

Support is added to the following features on the AP1552 models to be on par with the indoor APs:

- Local, FlexConnect, Monitor, Rogue Detector, and Sniffer modes
- VideoStream in Local mode
- HotSpot 2.0 in Local mode
- VoWLAN
- Band Select
- DTLS
- CleanAir of 5-GHz radio

Redundancy on Primary and Secondary Controllers

The term Redundancy in Prime Infrastructure refers to the high availability (HA) framework in controllers. Redundancy in wireless networks allows you to reduce the network downtime. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state, which continuously monitors the health of the controller in the Active state through a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing ordered unique device identification (UDI). A controller with redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.

Note The stateful switchover of clients is not supported, which means that all clients, with the exception of clients on locally switched WLANs on access points in FlexConnect mode, are deauthenticated and forced to reassociate with the new controller in the Active state.

Automated Deployment Profiles

The Prime Infrastructure Automated Deployment feature allows you to create templates that can be hosted on the Automated Deployment Gateway. Network devices (for example, ISR G2, Catalyst switches) with Cisco Networking Services (CNS) agents can call home to the Automated Deployment Gateway to pull their configuration templates down. After provisioning, the management of those devices follows the regular Prime Infrastructure process.

ScanSafe

ScanSafe Web Security is a cloud-based SaaS (Security as a Service) that allows you to scan the content of the HTTP and HTTPS traffic. When the ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to the ScanSafe cloud for content scanning and malware detection.

Important Notes

- The Cisco 12.2EWA IOS Image for Catalyst 4948 does not work properly. Cisco Prime Infrastructure supports IOS Image 12.2SG for Catalyst 4948 series. This is because of different sysOId's returned by Cisco IOS Images.
- For the TACACS+/RADIUS user authentication, the custom attributes related to the new features are required to be added/appended to the existing set of attributes in AAA server to access certain pages/views. For example, Monitor Media Stream page, Virtual Domain List (to view the list of virtual domains from the Create Report page), and so on. For RADIUS authentication and authorization in Prime Infrastructure 1.2, there is an alternate method available for the AAA users. Only the user role and virtual domain attributes can be configured in AAA server (instead of copying the complete custom attribute task list from NCS to the AAA server).

Open Caveats

Table 3 lists the Open Caveats in Cisco Prime Infrastructure Release 1.2.

Click the identifier to view the impact and workaround for the caveat. This information is displayed in the Bug Toolkit. You can track the status of the open caveats using the Bug Toolkit.

Table 3 Open Caveats

Identifier	Description
CSCtx58026	High Availability: Prime Infrastructure should be able to get a backup from the secondary before attempting a failback.
CSCua30266	There are differences in the number of "Authenticated Client Count" on Client Count report between "Report By: All" and "Report By: AP By Controller".
CSCua45107	With NCS 1.1.0.58, try to do auto-provision on a WLC 5508. When you choose a CSV file for MAC address, no error, but nothing is provisioned.
CSCua77597	Discrepancy in TX and RX data from client session report
CSCub01364	NCS tries all TACACS servers in the global list after receiving a reject

Table 3 Open Caveats (continued)

Identifier	Description
CSCub25487	The client session hourly report fails because of wrong calendar format.
CSCub34632	Permission Denied message appears for 'admin' user when trying to access the Audit report in NCS
CSCub38147	Prime Infrastructure does not show the Device Type for clients.
CSCub38682	BaseStation timestamp is incorrect.
CSCub41048	When accessing the Autonomous AP migration template page in NCS, an error occurs.
CSCub42183	WLC configuration backup fails on secondary to local FTP/TFTP.
CSCub43324	Session time attributes are not working.
CSCtu88206	If there are large number of sites and data sources in the **Administration > System Settings > Data Deduplication** page, browser displays "Unresponsive Script" message.
CSCtx94785	Change association in NAT 44, is not allowed for FastEthernet Interfaces.
CSCty97852	The Device Plug and Play does not happen after the Prime Infrastructure server is restarted or network connectivity is reestablished between PnP Gateway and the Prime Infrastructure server.
CSCtz96109	When cross-launching NAM through a web browser from PA server, the user might get a prompt in for entering user name and password, whereas the username and password should be taken automatically from the PA server
CSCua28691	The Device Type based deployment does not function when "cns id" other then UDI is used and "cns config initial <PnP Gateway hostname> <port> inventory" command is provided in the bootstrap configuration.
CSCub03050	Unable to delete third-party WLC from third-party device type category.
CSCub09942	The image is distributed and activated properly using UDI on device, but after device reloads the status of Image in Prime Infrastructure shows timeout failure and any config push after that also times out and fails.
CSCub21197	Report data are not generating based on the reporting period.
CSCub26014	Unable to deploy the VPN features using the composite templates.
CSCub36693	Deleting the WLAN or ACL should clear the mapping in Flex External webauth ACL.
CSCub50858	Cisco 3750E image wrongly recommended for plain 3750 from repository.
CSCtz77712	An error message appears when uploading new MIB in **Design > Custom SNMP Template > Upload MIB**. If the new MIB has references to MIB objects that are not uploaded first.
CSCua68559	Memory graphs do not populate for Nexus devices in Device Work Center.
CSCub74449	Creating Report fails as connection refused on 20566.
CSCub74721	In an upgraded setup, SWIM recommendation and import from CCO are not working because of login to CCO is failing in SWIM.
CSCub66826	If the username for proxy server contains "\" (domainname\username) then the Software Update page is unable to connect to Cisco.com
CSCua76425	After running the Conversation reports for first time with specific HostIP either in Source or Destination field, Application Filter and Datasource Filter entries do not populate.
CSCub62910	FNF extension parameters are added to Voice Video Data template are not propagated to reports. RTP conversations report will always show 0 as value for all RTP statistics columns (RTPSTAT1, RTPSTAT2 and RTPSTAT3).

Table 3 Open Caveats (continued)

Identifier	Description
CSCub66888	Deduplication enabled and auto detected sites, datasources and settings before upgrade did not retain after upgrade - it is disabled after upgrade.
CSCub66903	Device Data Sources has net flow device data and its status is up before upgrade, but after upgrade doesn't show the netflow device data and keeps on loading.
CSCub66911	Reports scheduling not retained after upgrade
CSCub67497	The Raw NetFlow reports not retaining after upgrade but when saved with same name it displays “report exists” and throws an error.
CSCub69059	An error occurs when user clicks 'run and save' on a custom FNF v5 report.
CSCub69257	In HA environment, creating a service on primary is not retained on the secondary server.
CSCub31324	When tried to remove/add default filter, it is creating duplicate filter option, which will affect filter operation and filter might not work properly.
CSCub72631	The non-default templates and custom FNF, SNMP templates will not be retained in upgrade, HA and Backup restore.
CSCub74751	Upgrade issues with alarms and inventory.
CSCub78719	Scroll bar is missing in the background task page.
CSCub80165	Client discovery fails if the controller has more than 20000 clients.
CSCua40683	When v9 and v5 template fields exactly match, the template will appear under v5 template folder.
CSCua58081	Flexible NetFlow extension parameters do not appear in Conversations reports.
CSCua83403	7600 device is shown as mediatrace capable in pathtrace UI but actually user cannot start media trace
CSCub56197	Running Mediatrace command over HTTPS is not supported for ASRs
CSCub79976	Intermittent issues with High Availability.
CSCub53867	Selected Image name for distribution is not getting populated for a few devices.
CSCub57144	Image import fails if the image size is large.
CSCub65427	Upgrade Analysis is not working for ASR series devices.
CSCub72156	DWC Image recommendation is not shown for a few device families.
CSCua57435	Unable to complete provisioning when triggered in virtual domain with user Admin.
CSCub60594	PnP provisioning is not getting completed when profile has only image.
CSCtz99807	The template deployment history is not refreshed.
CSCub36844	Templates with DB variables are not getting deployed on Devices properly, even though their status appear success
CSCub57283	Deployment of configuration templates fail when the device name is long
CSCub35534	Restore operation fails occasionally with RMAN exception
CSCub38566	Data Cleanup takes long time to finish
CSCua29756	Unknown exception occurs when launching saved reports on an upgraded NCS.
CSCub40295	Unable to import WLAN template
CSCub69051	An error occurs while accessing Web-Authentication and Web-Policy ACLs at AP level.
CSCub35142	Results shows incorrect client count when 11u option selected in dashlet

Table 3 Open Caveats (continued)

Identifier	Description
CSCua65828	Running a Combined Inventory Report fails with error "Failed to run report: Illegal setting for report: routers_by_model"
CSCua46786	Undeploy template which is mapped to another template fails without displaying the proper failure reason.
CSCub81156	Wired clients show up late after a re-sync in upgraded server
CSCub81158	Resync after upgrading Switch IOS not work
CSCub74871	After a synch operation, a few of the ISRs in managed state are getting into "Managed with Warnings"

Resolved Caveats

Table 4 lists the Resolved Caveats in Cisco Prime Infrastructure Release 1.2.

Click the identifier to view the details of the caveat. This information is displayed in the Bug Toolkit. You can track the status of the resolved caveats, using the Bug Toolkit.

Table 4 Resolved Caveats

Identifier	Description
CSCtx47086	Distribution fails when backing up image greater than 64 MB
CSCtx66256	Traps and syslogs do not update the switch interfaces status
CSCtx68254	Legacy import is not working for MAC Filter and Local net users template
CSCty09212	Object selector fails to get the data from device
CSCty10979	Device inventory details not retried by config
CSCty11000	Device tree throws RSL error when not connected to internet with Firefox 7
CSCtz16897	Buttons for the basic operations are disabled
CSCtz23103	Issues with Design view interfaces templates
CSCtz33408	SAM to use the threadpool than creating threads for CDB to Oracle
CSCtz34018	Device 360° view of the unified AP is not working.
CSCtz36156	Alarms do not send e-mail notifications
CSCtz36170	Devices managed with warnings with empty information
CSCtz46310	NAMs hostnames not in Device Work Center (DWC) and all the other (non-NAM) devices are discovered ' Managed with Warnings'
CSCtz47946	On scale starting 5 NBI clients caused Prime Infrastructure 1.2 to system unusable
CSCtz52708	Image Distribution and archive fails on NME-NAM, SRE-NAM and NAM3 devices.
CSCtz55083	Routing: Screen Hanging for: Multiple delete
CSCtz56573	All graphs should show host names instead of IP addresses
CSCtz56953	Image download 3560E and 6509 has no recommendations
CSCtz60367	Check for update with mockup server fails
CSCtz60731	Software update from Cisco.com is not working
CSCtz66454	SWIM Image recommendations is not working for any devices in NCS 1.1.1.

Table 4 Resolved Caveats (continued)

Identifier	Description
CSCtz72498	Service Engine interface duplication in interface table in database
CSCtz81115	The line chart presented on the Generic Dashlet currently displays only top 15 entries for Custom SNMP templates.
CSCtz81184	The Generic Dashlet table view only shows last 15 records.
CSCtz81909	Update: Problem while connecting to Cisco.com from the NCS server
CSCtz82220	Severity Configuration in Admin setting throws an exception
CSCtz83345	Disk allocation is incorrect for small OVA
CSCtz88702	Inventory collection of ASR devices failed
CSCtz90989	Unable to generate DMVPN reports
CSCua07924	Licensing Check from the Login page is not working correctly.
CSCua08058	Monitoring Object Selector disappears while creating Custom SNMP template.
CSCua14928	Performance: Logging into Prime Infrastructure takes more than three minutes
CSCua18416	GETVPN Group Member: Deploy is not pushing CLIs to router
CSCua22929	NCS Audit works incorrectly, VLAN deletion from the VLAN list is not reflected
CSCub29697	NCS stops collecting the client data
CSCub38551	database deadlock
CSCtw57789	Sorting function does not work in Unclassified/Malicious Rogue APs
CSCtw66822	addObjectsWithOverrideWithoutUpdate still calls validation
CSCtw75535	Virtual Domains not showing maps, WLCs, APs - DB corruption
CSCtw89250	Rx/Tx Utilization dashlet slider issues
CSCtw98787	ncs password ftpuser CLI command should enforce ftp-user parameter
CSCtx09586	"Copy And Replace AP" function does not work
CSCtx49184	FTP Login with HA enabled fails with 503 Error
CSCtz37295	Alarm summary panel displays an error for lobby ambassador login
CSCtz56558	Lobby admin gets to the NCS home page by hitting the browser back button
CSCtz76125	Repository create button doesn’t specify it wants ftp:// notation
CSCtz86275	Client throughput report not showing WLC hostname when chosen
CSCua06057	Consistent sort of AP columns at monitor and config pages
CSCua10735	NCS Client Reporting Engine (.CSV) Showing Wrong Stats
CSCua12065	NCS GPS markers discrepancy
CSCua15365	Count of Severity Configuration 263 is wrong
CSCua24736	MSE backup background task End Time and Elapsed Time are not correct.
CSCua30988	Riyadh timezone preventing NCS to start completely
CSCua34859	Unable to sync maps - the ORA-01400 error occurs.
CSCua42222	NCS autonomous AP client discovery fails
CSCua42719	NCS reports an unknown exception when importing a CSV file

Table 4 Resolved Caveats (continued)

Identifier	Description
CSCua43557	Heatmap issue when resizing the browser
CSCua44995	Port number ‘0’ is detected on AP associated event
CSCua46573	NCS Coverage Hole report not created
CSCua50117	NCS FTP server fails to open more than 4-6 concurrent FTP sessions
CSCua63402	NCS stops forwarding Northbound traps
CSCua71487	Protocol groups template are not saved when port ranges are configured
CSCua78651	NCS cannot delete WLC due to guest user account
CSCua89174	Changes in Settings > Data Management will not free up the disk space
CSCua90537	Alarms search filter should reset itself when browsing to another page
CSCua92870	Import AP config fails from NCS
CSCub02541	NCS is not collecting all the needed debug information when downloading log
CSCub03130	CleanAir report for interferes when exporting to CSV format does not show the Discovered or Last Updated time stamp.
CSCub05069	Critical Alarms are not available after migration
CSCub12524	Some traps in the NCS Northbound processing queue are being dropped
CSCub15467	NCS Client Summary by SSID export in CSV is broken
CSCub15735	default-group AP group template makes no sense in NCS
CSCub34733	4507R+E w/ Supervisor 6L-E shows as Unsupported Device in NCS
CSCua73343	HA Fallback failed resulted in Primary DB READ-ONLY mode
CSCub44418	After NCS is upgraded from NCS 1.1 to Prime Infrastructure 1.2, the Application Visibility feature should to be reconfigured.
CSCua89477	Disk usage alarms need to be improved
CSCub40799	Delete old backups
CSCub51737	ISR memory utilization shown by 360 is different from inventory details.
CSCua34353	Database grows causing out of disk space issue and causes services to stop running correctly.
CSCua89486	Review the user guide recommendations to use a small-medium-large ova
CSCtr92475	Oracle maximum connections exceeded

Related Documentation

You can access the following additional Cisco Prime Infrastructure documentation on Cisco.com:

- Cisco Prime Infrastructure 1.2 Quick Start Guide
- Cisco Prime Infrastructure 1.2 User Guide
- Cisco Prime Infrastructure 1.2 Configuration Guide
- Open Source Used In Cisco Prime Infrastructure 1.2
- Cisco Prime Infrastructure 1.2 Supported Devices

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.