Release Notes for Cisco Prime Infrastructure, Release 1.4

Last Updated: July 2013
OL-27652-06

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. Cisco 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.

Cisco 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/1.4/configuration/guide/pi_14_cg.html

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

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.4/quickstart/guide/cpi_qsg_1_4.html

Virtual Appliance - Hardware Requirements

For information about the number and type of devices supported by each virtual appliance size, see the Product Specifications section of the Cisco Prime Infrastructure 1.2 data sheet at http://www.cisco.com/en/US/products/ps12239/products_data_sheets_list.html.

Browser Support

Cisco Prime Infrastructure supports the following browsers:

- Google Chrome—25.0, 26.0 or 27.0
- Mozilla Firefox— ESR 17.x, 17.0 or later
- 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 Device Types and Software Versions

Table 1 lists the wireless devices and their software versions that are supported by Cisco Prime Infrastructure 1.4.

Table 1 Supported Wireless LAN 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	7.0 and later versions
Cisco Flex 7500 Series	7.0 and later versions
Cisco 8500 Series	7.3 and later versions
Cisco Virtual Controller	7.3 and later versions
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

Table 2 lists the Cisco Prime Infrastructure supported devices for switches, wireless LAN controllers, access point images, Identity Services Engine (ISE), and mobility services engines (MSE).

Table 2 Supported Device Matrix for Switches, WLC, MSE, ISE, and AP

Supported Switches	Supported Controllers	Supported MSE Devices	Supported ISE Devices	Supported Lightweight APs	Supported Autonomous APs
Cisco Catalyst 2960, 2975 Switches [Cisco IOS Release 12.2(50)SE], Cisco Catalyst 3560 Switches [Cisco IOS Release 12.2(50)SE], Cisco Catalyst 3750 Switches [Cisco IOS Release 12.2(50)SE], Cisco Catalyst 3850 Series Ethernet Stackable Switches Cisco Catalyst 4500 Switches [Cisco IOS Release 12.2(50)SG], Cisco Catalyst 6500 Switches [Cisco IOS Release 12.2(33)SXI], Cisco NAM 2304 Appliance, Cisco NAM 2320 Appliance, Cisco IE 2000 Series Switches.	Cisco 2100 Series Cisco 2500 Series Cisco 4400 Series Cisco 5500 Series Cisco Flex 7500 Series Cisco 8500 Series Cisco Virtual Controller Cisco WiSM Cisco WiSM2 Cisco Wireless Controller on Service Ready Engine (WLCM2 on SRE) Cisco Catalyst 3750G Series Integrated Wireless LAN Controllers	Cisco MSE 3355	Cisco ISE 1.0 Cisco ISE 1.1	Cisco 600 Series, Cisco 1040 AP, Cisco 1100 AP, Cisco 1120 AP, Cisco 1130 AP, Cisco 1140 AP, Cisco 1200 AP, Cisco 1230 AP, Cisco 1240 AP, Cisco 1250 AP, Cisco 1260 AP, Cisco 1500 AP, Cisco 1524 AP, Cisco 1552C AP, Cisco 1552CU AP, Cisco 1552E AP, Cisco 1552EU AP, Cisco 1552H AP, Cisco 1600e AP, Cisco 1600i AP, Cisco 2600i AP, Cisco 2600e AP, Cisco 3500i AP, Cisco 3500e AP, Cisco 3500p AP, Cisco 3600i AP, Cisco 3600e AP, Cisco 3600p AP, Cisco 700i AP, Cisco 700e AP, Cisco 802agn AP, Cisco 802gn AP, Cisco 802hagn AP, Cisco 801gn AP, Cisco 801agn AP	Cisco 1130 AP, Cisco 1141 AP, Cisco 1142 AP, Cisco 1200 AP, Cisco 1240 AP, Cisco 1250 AP, Cisco 1260 AP, Cisco 1800 AP, Cisco 800 ISR Series, Cisco Aironet 1310 and 1410 Bridges, Cisco 2600 AP, Cisco 3500 AP, Cisco 3600 AP, Cisco 1600 AP, Cisco 801 AP, Cisco 1100 AP

For 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

For detailed information on the Cisco MSE Virtual Appliance Product Specifications, see the following URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c78-475378.html

Installation Guidelines

For detailed installation information, see the following Cisco Prime Infrastructure Guides:

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.4/quickstart/guide/cpi_qsg_1_4.html#wp69980

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps12239/deployment_guide_c07-721232.html#wp9000555

Upgrading Cisco Prime Infrastructure

Important Notes

- We recommend that you upgrade to Prime Infrastructure 1.4 only if you are deploying AireOS WLC 7.5 release.
- Once you upgrade to Prime Infrastructure 1.4, you may not be able to upgrade to some new versions of Prime Infrastructure at the time of their release. However, a migration path will be made available for the latest available version of PI at a later date.
- We highly recommend that you take a backup of your data before upgrade and save it for the future.
- If you are running the previous releases of Prime Infrastructure such as 1.1.0.58, 1.1.1.24, 1.2.1.12 and not planning to upgrade to Prime Infrastructure 1.4, it is recommended to upgrade to Prime Infrastructure 1.3.0.20 and apply the upgrade patch (Update 1 for Cisco Prime Infrastructure 1.3.0.20). For more details, see Release Notes for Update 1 for Cisco Prime Infrastructure 1.3.0.20.
- You cannot migrate from Cisco WCS 7.x to Prime Infrastructure 1.4. If you want to do this, you need to follow instructions to migrate to 1.1.1.24 and then upgrade to Prime Infrastructure 1.4. For more information, see the following URL:
  http://www.cisco.com/en/US/docs/wireless/ncs/1.1/release/notes/NCS_RN1.1.1.html
- Different point patch files are provided for each version of Prime Infrastructure predecessor products. If you need help applying a point patch to your existing system before you start any upgrade to Prime Infrastructure, read the Installing the Point Patch section of the *Cisco Prime Infrastructure 1.4 Quick Start Guide*.

Recommended Upgrade Paths

- You can upgrade the following products to Cisco Prime Infrastructure 1.4:
- Cisco Prime Network Control System 1.1.0 (1.1.0.58)
- Cisco Prime Network Control System 1.1.1 (1.1.1.24)
- Cisco Prime Infrastructure 1.2.1.12
- Cisco Prime Infrastructure 1.3.0.20
- Update 1 for Cisco Prime Infrastructure 1.3.0.20
- If you are running the previous releases of Prime Infrastructure such as 1.1.0.58, 1.1.1.24, 1.2.1.12 and not planning to upgrade to Prime Infrastructure 1.4, it is recommended to upgrade to Prime Infrastructure 1.3.0.20 and apply the upgrade patch (Update 1 for Cisco Prime Infrastructure 1.3.0.20). For more details, see Release Notes for Update 1 for Cisco Prime Infrastructure 1.3.0.20.
- You cannot migrate from Cisco WCS 7.x to Prime Infrastructure 1.4. If you want to do this, you need to follow instructions to migrate to 1.1.1.24 and then upgrade to Prime Infrastructure 1.4. For more information, see the following URL:
  http://www.cisco.com/en/US/docs/wireless/ncs/1.1/release/notes/NCS_RN1.1.1.html
- Once you upgrade to Prime Infrastructure 1.4, you may not be able to upgrade to some new versions of Prime Infrastructure at the time of their release. However, a migration path will be made available for the latest available Prime Infrastructure at a later date.

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

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.4/quickstart/guide/cpi_qsg_1_4.html#wp56675

Submitting Feedback

Your feedback will help us improve the quality of our product. To send your feedback, follow these steps:

Step 1 If you have configured your mail server, go to Step 8.

Step 2 Choose **Administration > System Settings > Mail Server Configuration**.

Step 3 In the Mail Server Configuration page, enter the mail server details.

Step 4 Click **Save** to save the configuration settings.

Step 5 Choose **Help > Help Us Improve Cisco Products**.

Step 6 In the Help Us Improve Cisco Products page, select the **Yes, collect data periodically** option.

Step 7 Click **OK**.

Step 8 Choose **Help > Submit Feedback** (in the Classic view) or click the question mark icon at the top right and then click **Submit Feedback** (in the LifeCycle view).

Note You must configure the e-mail server and then enable data collection to configure the feedback tool.

Cisco Prime Infrastructure License

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

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

Cisco Prime Infrastructure 1.4 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 1.4:

Management Support for WLC Release 7.5

Prime Infrastructure 1.4 provides management support for WLC Release 7.5 and associated features. In addition, this release provides support for AP platforms such as 3600P and 802.11ac module.

For more information about Cisco Unified Wireless Network (CUWN) Software Release 7.5, see the product bulletin at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2797/prod_bulletins_list.html

For more information about the features of WLC Release 7.5, read the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.5* available at the following URL:

http://www.cisco.com/en/US/products/ps10315/prod_release_notes_list.html

Support for 802.11ac Module

This release provides management support for 802.11ac module—a field-upgradable add-on module to the AP 3600. The 802.11ac module for the 3600E or 3600 AP allows customers to deploy 802.11ac in an enterprise using their existing AP 3600. AP3600 maintains dual-band support 2.4 and 5 GHz, supporting b/g/n on 2.4 GHz and a/ac/n on 5 GHz. Prime Infrastructure 1.4 provides support for configuration and monitoring of the main radio and the module radio (support for additional configuration such as channel width, DCA, and MCS).

Support for Cisco AP 700

This release supports Cisco Aironet 700 Series Access Point. This is an affordable compact dual-radio access point for value-minded customers looking to modernize your networks to handle today's increasingly complex wireless access demands.

Policy Classification Engine

The controller can do profiling of devices based on protocols such as HTTP, DHCP, and so on to identify the clients. You can configure device-based policies and enforce per-user or per-device policy on the network. The controller also displays statistics that are based on per-user or per-device end points and policies that are applicable to a device.

Detect Dead Radios

In this release, the report feature is enhanced in such a way that you can choose the Dead Radios option for inventory reports to show the APs which are not operational. That is, the APs whose Admin status is “Up” and operational status is “Down”.

FlexConnect Audit Support

In the FlexConnect deployment mode, APs can survive a controller outage by going into a standalone mode. This is different from the centralized mode in which many configuration items are stored at the AP. For example, if you are performing a routine configuration audit for all the stores that were recently upgraded to the FlexConnect architecture, you need to make sure that all of the APs at the store have received the correct FlexConnect group and that they are mapped to the correct VLAN. You should also ensure that all WLANs active in the store are using the correct security profile.

We recommend that you use WLAN in enabled state to avoid audit mismatches at WLAN-VLAN Mappings at the FlexConnect AP.

Autonomous AP Support

Image upgrade is supported for Autonomous AP in PI 1.4 and the following new Autonomous AP platforms are supported in PI 1.4:

- AP2600 - AP3G2 Image Family and Image Version 15.2.2-JA(ED)
- AP3500 - AP3G1 Image Family and Image Version 12.4.25d-JA2(ED)
- AP3600 - AP3G2 Image Family and Image Version 15.2.2-JA(ED)
- AP1600 - AP1G2 Image Family and Image Version 15.2.2-JB(ED)

Client Stateful Switchover (SSO)

In wireless Client SSO, the client state is also maintained on the Active and Standby WLCs, and the wireless clients are not de-authenticated after switchover.

Cable Modem Monitoring

The CMTS is a Cisco Universal Broadband Router (uBR) which enables communication with a Hybrid Fiber Coaxial (HFC) Cable network via a Cisco MCxx cable modem card. Cisco MCxx cable modem cards allow you to connect cable modems on the HFC network to a Cisco uBR7200, uBR7100 or a uBR10k in a Community Antenna Television (CATV) headend facility. The modem card provides the interface between the Cisco uBR protocol control information (PCI) bus and the radio frequency (RF) signal on the DOCSIS HFC network. While service providers continue to use CMTS to manage the cable modem, they can to monitor key cable modem health parameters using Prime Infrastructure.

Support for SFTP

This release enables you to use the Prime Infrastructure server as a Secure File Transfer Protocol (SFTP) server for which you need to create an SFTP user. You can add an SFTP server as an external server in Prime Infrastructure. Also, you can use File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) and Secure File Transfer Protocol (SFTP) while uploading and downloading files to and from Prime Infrastructure.

Important Notes

- The Cisco IOS 12.2EWA image for the Cisco Catalyst 4948 does not work properly. Cisco Prime Infrastructure supports the Cisco IOS 12.2SG image for the Cisco 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 the AAA server to access certain pages/views. For RADIUS authentication and authorization in Prime Infrastructure 1.3.0.20, there is an alternate method available for the AAA users. Only the user role and virtual domain attributes can be configured in the AAA server (instead of copying the complete custom attribute task list from Prime Infrastructure to the AAA server).
- After performing a major version upgrade of the Cisco Prime Infrastructure application, the browser cache on the client machines used to access the older version need to be cleared once so that the data for the old application is removed from the browser cache. Afterward connecting to the upgraded server works fine.
- SWIM Image Management and Supported Devices—Table 3 provides a brief overview about the different processes involved in managing software images and whether the processes are supported in the Unified Wireless LAN Controllers and devices.

Table 3 Software Image Management Processes and Supported Devices

Software Image Management Processes	Description	Unified WLCs	Cisco Catalyst 3850 Switches (Cisco IOS XE 3.2.1)
Image import from device	Ability to import software image from devices that are already deployed to Cisco Prime Infrastructure. The software image can then be distributed to other devices.	Not supported because the software image cannot be reassembled into a package.	Supported
Image import from file	Ability to import software image from known location on a file server to Cisco Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported
Image import from URL	Ability to import software image from network accessible locations (URI/URL) to Cisco Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported
Image import from Cisco.com	Ability to import software image from a trusted Cisco website to Cisco Prime Infrastructure. The software image can then be distributed to other devices.	Supported	Supported
Image upgrade/distribution	Ability to upgrade software image on the managed devices from Cisco Prime Infrastructure. This allows you to update software image for multiple devices based on demand or at a later point in time as scheduled. The feedback and status are displayed during the upgrade and devices can be restarted, if required. In large deployments, you can stagger reboots so that the service at a site is not completely down during the upgrade window.	Supported	Supported

Table 3 Software Image Management Processes and Supported Devices (continued)

Software Image Management Processes	Description	Unified WLCs	Cisco Catalyst 3850 Switches (Cisco IOS XE 3.2.1)
Image recommendation	Ability to recommend a compatible image for the devices that are managed from Cisco Prime Infrastructure.	Not supported because the flash requirement is not available.	Supported
Image upgrade analysis	Ability to analyze the software images to determine the hardware upgrades required before you can perform the software upgrade.	Not supported because there is no minimum requirement for RAM or ROM. The newly upgraded image replaces the existing image after an upgrade.	Supported

- SWIM and Configuration Archives support for Devices during Cisco Prime Infrastructure releases—Table 4 outlines the devices that the software image management and configuration archives support during the various Cisco Prime Infrastructure releases.

Table 4 SWIM and Configuration Archives support for Devices during Cisco Prime Infrastructure Releases

Devices	Cisco Prime Infrastructure releases
Cisco 4400 Wireless LAN Controller[1]	1.2, 1.3, and 1.4
Cisco 5500 Series Wireless LAN Controllers	1.2, 1.3, and 1.4
Cisco WiSM1 Controller	1.2, 1.3, and 1.4
Cisco 2106 Wireless LAN Controller[1]	1.2, 1.3, and 1.4
Cisco 2504 Wireless LAN Controller	1.2, 1.3, and 1.4
Cisco 2800 and 3800 Series Integrated Services Routers	1.2, 1.3, and 1.4
Cisco Flex 7500 Series Wireless LAN Controller	1.2, 1.3, and 1.4
Cisco 8500 Wireless LAN Controller[1]	1.4
Cisco Virtual Wireless LAN Controller[1]	1.4
Cisco WiSM2 Controller	Not supported

1. PI 1.4 does not support SWIM in Cisco 2106/4400/8500/WiSM2/Virtual WLC.

Open Caveats

Table 5 lists the Open Caveats in Cisco Prime Infrastructure Release 1.4.

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 5 Open Caveats

Identifier	Description
CSCua30266	Inconsistency in the number of "Authenticated Client Count" reported in the Client Count report, if the selected time period is beyond one day.
CSCua77597	Discrepancy in client session traffic report and report generated by Cisco accounting software/third party tools.
CSCua81340	Controller Configuration Groups fail to display controllers correctly.
CSCub42183	In HA deployment mode, the backup fails when you run "Controller Configuration Backup" task with repository set to either local TFTP or FTP.
CSCub49713	If the backup-staging-url is the same as the nfs repository, the resulting backup gets deleted when the cleanup is done for the staging URL.
CSCuc25021	In HA setup, firewall settings will not be updated properly on reboot.
CSCuc25038	The state value in HA config file on secondary server is not updated due to which the secondary server fails to start.
CSCuc43987	Unable to delete switches from NCS 1.1.1.24 OVA appliance.
CSCuc45245	In PI 1.2, in some instances the background map image is missing.
CSCuc46116	PI cleanup deletes control file.
CSCuc51669	Unable to view Rogue AP's location in the Alarms Page.
CSCuc55283	The alarm generated does not have the IP Address of the requester whose authentication failed.
CSCuc56004	When you run the command "ncs cleanup" after the patch install, all services except the database services are started.
CSCuc59023	In PI 1.2, device groups are not populated when you upgrade from NCS 1.x.
CSCuc74807	In the LifeCycle view, the Deploy configuration page takes long time to load.
CSCuc89874	PI stops responding while trying to import DWG.
CSCud15241	TFTP connection fails when IPTABLES is enabled.
CSCud15404	After PI 1.2 upgrade to PI 2.0, http web certificate missing on server...
CSCud26027	Occasionally, PI server will stop responding to GUI requests due to OutOfMemoryExeception (OOM event).
CSCue21462	Unable to delete Cisco Aironet 1240 AP from inventory after restoring the backup image.
CSCue37536	PI cannot complete all the required background tasks when a statistics table space in the database is full.
CSCue47128	When an accesspoint is added to a map, it automatically goes to position AP page. Before the positioning page is launched, if zoom is done, then on position AP page, only the first AP is draggable. Selecting other AP does not unselect the first AP.
CSCue60499	When you configure Rogue AP Rules template from the classic theme, you cannot apply the template to the controllers, as "Apply to Controllers" button does not to work.
CSCue66897	The Quick Search tool takes a longer time to respond.

Table 5 Open Caveats (continued)

Identifier	Description
CSCue70798	When removing the variables from the existing CLI Configuration Template, the operation is successful, but when browser is refreshed the variable is visible again under "managed variables".
CSCue76386	In life cycle view, duplicate site groups are displayed in DWC view after restoring PI database.
CSCuf11576	In PI 1.3 Life Cycle View, navigate to Design> External Management servers > ACS View servers. The selected tab button on the top moves from Design to Deploy.
CSCuf37583	Backup fails when you use SFTP as the protocol for PI repositories.
CSCuf55547	In PI 1.3, config archive fails for Virtual WLC.
CSCuf65530	When you upgrade from NCS 1.1 to PI 1.3, all SNMP and telnet/SSH credentials are correct, but the status of the controllers are shown as "managed with warnings".
CSCuf74214	Plug n play does not work in PI 1.4 upgraded setup due to issue with message broker configuration in messaging.properties.
CSCuf77712	DWG to PNG file conversion shows partial image.
CSCug07178	PI 1.4 server restored with SSO data gets redirected to the backup server.
CSCug25451	In Classic view, you cannot sort the templates listed under Configure > Controller Template Launch Pad > WLANs > AP Group.
CSCug31560	PI adds MGMT interface MAC address instead of Burned In Address (BIA) for mobility group member.
CSCug34809	When you create and save a custom SNMP template, it is not clear where the template is actually saved.
CSCug34820	The functions available in Design> Monitoring Configuration> Templates> Features> Custom SNMP page, are unclear.
CSCug35324	When you restore NCS 1.1.1.24 backup on PI 1.2, the Deploy > Configuration Tasks page does not get loaded for the first time. You have to launch the page multiple times to view the data.
CSCug37165	After you restore PI 1.3 backup server to PI 1.4 restored server, "Local interface IP" shows the backup server IP instead of restored server IP. Also, you will not be able to login with RADIUS or TACACS credentials.
CSCug40106	The "state" field of Rogue AP reports in PI is unreliable.
CSCug53428	After image upgrade operation, the Cisco Cat3750x device boots up with old image rather than the newly loaded image.
CSCug61312	False alarms are generated for few rogue APs.
CSCug70014	Some reported statistics from Pi are incorrect.
CSCug82400	Obsolete WSSI radio interface in PI.
CSCug98099	When deploying CLI template from lifecycle view in PI 1.2.1, the job fails
CSCuh20025	The widgets on floor maps in PI throws exceptions and does not display the expected data.

Table 5 Open Caveats (continued)

Identifier	Description
CSCuh47572	Incorrect Multicast IP address for a particular Mobility Group object is displayed in Controller->System->Multicast page.
CSCuh51895	PI recognizes valid wireless APs as rogue AP by wIPS.
CSCuh60995	SM-SRE image file import fails.
CSCuh61007	When you select an image and distribute on SM-SRE device, distribution does not proceed, and an error an displayed.
CSCuh62796	SWIM distribution fails for NAM patch.
CSCuh65513	Custom NeftFlow report instance does not show any data.
CSCuh79507	APs in maintenance mode will trigger critical alarms, even if you set low severity for AP Disassociation events.
CSCug83205	Image copy is successful but the reload does not take place with a new image.
CSCuh66190	Image recommendation fails for three device types.
CSCui32574	Unable to import image for Cisco Catalyst 3850.
CSCui17662	The location information for wIPS Attack alarms is missing.
CSCui37076	Lag support unavailable for WLC 2500 in the templates/configuration pages.

Resolved Caveats

Table 6 lists the Resolved Caveats in Cisco Prime Infrastructure Release 1.4.

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 6 Resolved Caveats

Identifier	Description
CSCty21268	NCS 1.1.0.58 cannot modify WLC 5508 dynamic interface IP Address.
CSCtz33783	Unable to open EAP-FAST parameters on adding legacy controllers.
CSCua45107	Auto-provisioning on a controller through CSV file for MAC address fails.
CSCua61592	.11b/g/n radio shown as 5.8 GHz.
CSCua98801	Error occurs during creation of Global CDP configuration.
CSCub18190	On upgrading from PI 1.2 to PI 2.0, you will see issues with AAP Inventory background task and multiple entries for single AAP.
CSCub35534	Restore fails with RMAN exception (RMAN-00571) due to missing log files.
CSCub38682	BaseStation timestamp is incorrect.
CSCub40295	Unable to import WLAN, FlexConnect, AP Group TEMPLATE in PI 1.2.
CSCub41299	ACL counters does not work when migrating from WCS 7.0.230 to NCS 1.1.
CSCub42415	Unable to save monitor settings in NCS Admin.
CSCub48331	PI CCO recommendation images not listed for many device families.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCub54769	Quick search returns error message.
CSCub57077	HA registration fails.
CSCub72534	In HA setup, there are issues with instance directory creation and package properties.
CSCub91535	Template push/refresh config fails.
CSCuc06938	PI Clients and Users page keeps loading if WLC interface is named as 'null'.
CSCuc09499	Permission is denied for admin users, when you log into MSE Northbound Notifications page.
CSCuc21532	Unable to add Controller to PI, after auto-install.
CSCuc28074	Controller > Mgmt Frame Protection page fails to come up.
CSCuc29378	PI 1.2 fails to start after a database restore from NCS1.1.1.24.
CSCuc42993	"Refresh from network" fails when Autonomous AP is present on the floor.
CSCuc57064	NC2.0:Exception when creating maps with floor area
CSCuc58999	Client does not show up on PI dashboard.
CSCuc59539	NCS2.0:OutofMemory error created and NMSserver Gets stopped.
CSCuc74852	Jobs Dashboard page reports error and does not display the jobs list.
CSCuc78802	Autonomous AP IOS image download using FTP fails due to blank FTP password.
CSCuc84305	PI service fails and cannot be restarted.
CSCuc88877	Blank screen appears when you launch license pop from PI About window.
CSCuc94865	Background task Autonomous AP Operational Status takes longer time to get started.
CSCud03122	PI 1.2 root account gets deleted after upgrade.
CSCud03240	Method getCorrelationAlertInfoForAps should not be called for Autonomous APs.
CSCud06139	backup.sh should check for space under /opt/backup if it exists.
CSCud06152	Alarm summary window opens behind floor map.
CSCud06695	Advance search page for APs and Clients are partially displayed.
CSCud07718	Network Device Summary shows wrong PIE chart for AP availability.
CSCud08265	PI background task does not progress.
CSCud13246	Advance search does not work properly.
CSCud16028	Assurance license pop up appears even after adding permanent license in PI 1.3 and upgrading to PI 1.4.
CSCud24761	Unable to create device groups for existing locations.
CSCud33269	PI requests for username/password for devices. This device requires no username and passwords.
CSCud39395	Mismatch between RMAN Archive logs and disk contents causes database crash.
CSCud39833	"Update and Sync" functionality does not work on unmanaged devices.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCud40312	Adhoc Rogue severity is categorized wrongly in PI.
CSCud45623	Devices are not displayed while creating Virtual Domain.
CSCud48173	Opening any AP protocol (802.11b/g/n,802.11a/n) throws error.
CSCud48564	Guest user account generates wrong password.
CSCud49730	No data available in Interface License Manager page.
CSCud51139	After upgrade, db_recovery_file_dest_size becomes full and database doesn't start.
CSCud57234	Catalyst 3850 switch gets stuck in sync state after changing role from MC to MA.
CSCud61799	PI 1.2 monitoring fails with SNMP v3.
CSCud62096	TACACS authentication takes time due to the delay in XMP module.
CSCud62644	Error occurs while accessing maps.
CSCud64318	C2960S switch does not show VLAN data due to XML error.
CSCud75413	XMP Poller causes memory leak and high memory usage during processing.
CSCud80157	HA registration fails.
CSCud83646	In HA setup, monitoring templates are not displayed in failed back primary server.
CSCud92758	SNMP v3 AuthPriv Mode is not supported through SWIM in PI 1.2.
CSCud94275	Backup job does not pre-calculate disk space and informs user of the shortfall.
CSCud98783	The backup file (*.gpp) is not optimized.
CSCud98831	Rogue Access Point page shows wrong AP position when configured in meters.
CSCue00087	Error occurs while configuring OEAP600 AP in NCS1.2.
CSCue04038	Search does not work on APs.
CSCue10155	APTILO Export filename does not comply with WCS convention.
CSCue14047	Failure in restore process causes failure in data cleanup process.
CSCue17090	Time taken to display the previously designed floor details in the planning mode window is high.
CSCue18967	Fails to apply a CLI template from NCS 1.2.1.012 to the WLC.
CSCue19300	Unable to save Site Map Properties.
CSCue21189	Adding AP to map takes longer time.
CSCue21751	Restore upgrade from PI 1.1.1.24 to PI 1.2.1 fails
CSCue23814	PI 1.2.1 fails to start after restoring PI 1.1 database.
CSCue28644	Heatmap does not align itself correctly with the AP.
CSCue29770	Upgrade of the database from NCS 1.1.1.24 to PI 1.2.1.12 fails during the data manipulation.
CSCue35666	Oracle recovery area filling causes PI to stop and not restart.
CSCue36709	Device events page keeps loading forever.
CSCue40570	Unable to launch Google Earth map using Chrome browser in PI 1.3.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCue41023	The enable command does not work in the CLI template.
CSCue45427	PI 1.2 does not retain the interface created for dynamic interface templates.
CSCue46682	Existing HA settings of AP gets corrupted while applying AP template.
CSCue48865	Template Deploy Scheduler does not work for PM time entry.
CSCue48982	RFPrediction runs into out of memory.
CSCue49264	Login and Licensing pages are very slow if MSE device is unreachable.
CSCue49514	Restore of NCS backup file fails.
CSCue60672	PI is unable to create backup file at times.
CSCue71859	PI 1.3 does not accept the distance value as one while creating a new context aware notification event definition.
CSCue72580	PI does not support access point locations greater than 80 characters.
CSCue76428	PI client count report fails with 'no data found' for SSID's.
CSCue76606	Assurance dashlets are empty after restore from PI 1.2.1 to PI 1.3.0.
CSCue77191	PI 1.2 does not support NMSP configuration.
CSCue82602	For wired clients, the updatetime in database gets reset to zero.
CSCue83215	Refresh does not detect disassociated Aps.
CSCue87691	GetDevices API returns a max of 20 devices.
CSCue88410	VoWLAN NCS reset button does not work for Voice Audit.
CSCue89592	Unable to auto place the APs on the floor map in the planning mode.
CSCue92213	Alarms fails to load in PI 1.4 upgraded setup.
CSCue92994	RADIUS AV-Pair issues in PI 1.3.
CSCue93505	Oracle in PI creates an unlimited number of files.
CSCue94095	Misleading error message "Invalid backup file version exception: error" in PI.
CSCue98565	Out of disk space condition causes deletion of files such as .PNG and .GIF files and so on.
CSCuf02486	Unable to create dynamic interface on Redundancy enabled controller.
CSCuf06505	On switching from lifecycle to classic view, the chrome browser stops responding.
CSCuf06576	No rogue AP rules details are shown in config page of 7.5 WLC.
CSCuf07903	HA registration fails after restoring secondary backup in primary server.
CSCuf08221	PI runs out of memory due to time delay of 50 to 100 milliseconds per PDU.
CSCuf08691	PI map does not show Rogue AP, whereas Monitor > Alarms page shows Rogue AP.
CSCuf09135	In PI 1.3, access to Online help is denied for admin users.
CSCuf16427	PI 1.3 does not have the LAG option for WLC 8500 model.
CSCuf17394	Wrong CXF Jar loaded in PI 1.2 and 1.3.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCuf24095	Unclear messages are displayed when non root domain users change the map properties.
CSCuf34805	PI discovers even the unmanaged clients that are connected to neighboring switches/WLC as wired client.
CSCuf35380	A note on the tasks that have to be performed after changing the IP Address of PI server is not available in IP Address change section.
CSCuf51821	LUMOS application does not get installed with PI 1.4.0.13.
CSCuf55719	PI displays the link down detection without Port number and device IP Address.
CSCuf60680	SNMP error occurs while applying WLAN with L3 WebAuth security policy on 7.5.1.18 controller.
CSCuf65113	Long term data does not appear for most of the dashlets.
CSCuf65624	Unable to create an interface from config page.
CSCuf85131	Dashlets and reports does not populate data in 1.4 UBC restored server.
CSCuf85566	Catalyst 3850 switch distribution fails in PI 1.4 with reboot option.
CSCuf86195	New AP discovery takes longer time
CSCuf90180	Dashlets does not populate wireless data when you restore PI 1.2.1.12 on PI 1.4 server.
CSCuf90356	SyslogHandler flooded ncs*.log with error messages.
CSCug05038	Maps are not visible after an upgrade from some version of NCS to PI 1.3.0.20 .
CSCug09098	Unable to fill WLAN configuration details in Configure > Controller Template Launch Pad > WLANs > WLAN Configuration page.
CSCug10236	Inline upgrade from PI 1.4.0.15 to PI 1.4.0.16 does not proceed.
CSCug13322	In the Device Work-Center, the Zone-Based-Firewall, Application-Visibility and NAT configuration windows cannot be used for configuration.
CSCug17718	PI 1.3 is unable to save Flexconnect VLAN mappings on AP template.
CSCug20125	Basic search does not work in S&P server.
CSCug25355	HA secondary setup gets stuck because the appliance is not connected to the network.
CSCug27295	Report triggers error when called from NBI.
CSCug29723	PI adds incorrect mac address for mobility group members.
CSCug32448	Time taken to read from the Oracle database is too long thereby causing latency.
CSCug37051	Dashlets and reports does not populate NAM and netflowdata in PI 1.4 upgraded server.
CSCug39388	Mismatch found with respect to Central DHCP when AP mode is changed from local to flex.
CSCug39406	Mismatch found with respect to Central DHCP when AP is moved across AP Groups.
CSCug43926	PI does not display the MSE License Usage Table.
CSCug44027	Various wireless reporting issues due to dataset size.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCug44407	Changing the Aspect Ratio values does not change the image size on the map.
CSCug44863	Disabling radio on AP leads white noise around AP on air quality heatmap.
CSCug50356	Virtual Domain switching does not happen.
CSCug53879	OOTB and Discovered Folder is empty and do not have any templates.
CSCug57534	Multiple e-mails sent for tracked clients.
CSCug60715	Restore of PI 1.3 NEC backup on PI 1.3.0.20 fails.
CSCug62010	Deletion of restored template fails.
CSCug62380	NBI regression error.
CSCug62567	AP 802 does not generate heatmap in PI 1.3.
CSCug63532	Unjoined AP list is empty.
CSCug64140	Unable to add Controller specific AAA server using WLAN Template.
CSCug67712	In PI 1.3, error occurs during backup and also control file goes missing.
CSCug71184	Unable to add AVC profile in PI classic and life cycle theme modes.
CSCug72223	Flash stops responding on the main page.
CSCug72758	Control Path between the mobility members stays down.
CSCug74684	Monitor deployment does not work for managed devices.
CSCug77918	In PI 1.3, SNMP generic monitoring templates display negative values as zero.
CSCug78400	Error occurs while adding or replacing a floor image by DWG file.
CSCug78551	Offset in actual map while repostioning AP after upgrade.
CSCug78869	PI 1.3 continues to use SNMPv3 for health monitoring even after changing to SNMPv2.
CSCug79550	Restore fails in PI 1.3 server when there is an inconsistency/expired oracle archived logs in the backup file.
CSCug80248	APs in maintenance mode cause repeated entries in Access Point page.
CSCug80687	PI 1.3 scheduled MSE backup fails due to insufficient disc space.
CSCug83480	Issues with background task and WLC license.
CSCug85933	Audit mismatch on PI after deletion of a WLAN.
CSCug90929	PI 1.3 Update 1 gets stuck while providing CLI templates to controllers.
CSCug95851	Switchport tracing does not work across L3 boundaries.
CSCug96223	Restore on fresh Beta 2.0-197 large/standard OVA server fails.
CSCug96642	AP 802 does not generate heatmap in PI 1.3
CSCuh04019	In PI 1.3 Update 1, flash does not respond in RRM dashboard.
CSCuh09318	Homeview/Dashboard does not display the uptime of the controllers.
CSCuh14198	WLAN ID and SSID mismatch.
CSCuh14909	Autonomous AP added to PI are displayed as unknown devices and are not working.
CSCuh16757	Virtual interface missing in PI 1.3 Classic View.

Table 6 Resolved Caveats (continued)

Identifier	Description
CSCuh17946	PI creates a group template with an invalid port number.
CSCuh33585	APs on the map edge does not show on the printed map.
CSCuh62158	High CPU utilization causes third party library issue.

The bugs resolved in this release provide the following key functions:

- Enables pre-backup check - Checks database memory target and swap memory as part of signature file validation.
- Provides error handling capabilities during the restore process.
- As part of improvements to the backup, a signature file has been added in this release. The signature file is used during restore operation for further validation prior to restore so that failures can be avoided. Also, improvements have been made in reducing the backup size. The signature file provides the following key features:
  - Restore of the backup from larger OVA on to a smaller OVA would be restricted immediately instead of failure occurring during later stages of the restore process.
  - Any backup file created from an unsuccessful backup will have Bkp_Status in signature file as FAILED. This attribute is used by the restore to detect error immediately instead of failure occurring during the later stages.
  - Recorded Bkp_DB_Size attribute in the signature file is used for better disk space validation on restore. If the required space indicated in Bkp_DB_Size is unavailable, then restore operation is aborted immediately.

Related Documentation

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

- Cisco Prime Infrastructure 1.4 Quick Start Guide
- Cisco Prime Infrastructure 1.4 Configuration Guide
- Cisco Prime Infrastructure 1.2 User Guide
- Open Source Used In Cisco Prime Infrastructure 1.2
- Cisco Prime Infrastructure 1.4 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.