Release Notes for StarOS™ Software Version 21.9.0 and Ultra Service Platform Version 6.3

First Published: July 31, 2018
Last Updated: July 31, 2018

Introduction

This Release Notes identifies changes and issues related to this software release. This release is the next major feature release since 21.8.0/N6.2.0.

Release Package Version Information

Software Packages	Version
StarOS packages	21.9.0, build 69977
Ultra Service Platform ISO	6_3_0-5682
usp-em-bundle*	6.3.0, Epoch 3697
usp-ugp-bundle*	21.9.0, build 69977, Epoch 3746
usp-yang-bundle	1.0.0, Epoch 3587
usp-uas-bundle	6.3.0, Epoch 3770
usp-auto-it-bundle	5.8.0, Epoch 3794
usp-vnfm-bundle	4.2.0.74, Epoch 3689
ultram-manager RPM*	2.1.0, Epoch 238
USP RPM Verification Utilities	6.3.0
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

Refer to the Release Change Reference for a complete list of feature and behavior changes associated with this software release.

Related Documentation

For a complete list of documentation available for this release, go to:

- StarOS: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html
- Ultra Gateway Platform (including the Ultra M Solution): https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html
- Ultra Automation Services: https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html
- Virtual Packet Core (including VPC-SI and VPC-DI): https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Ultra M Hyper-Converged Model Component Versions

HW	SW	5.7	5.8	6.0	6.1	6.2	6.3
	StarOS	68173	68415	21.6.0, Build 68695	21.7.0, Build 68897	21.8.0, Build 69296	21.9.0, Build 69977
	ESC	3.1.0.116	3.1.0.116	3.1.0.145	3.1.0.145	4.0.0.104	4.2.0.74
	RH Kernel	7.3	7.3	7.3	7.3	7.4	7.5
	OSP	10	10	10	10	10	10
UCS C240 M4S SFF (NFVI)	BIOS	3.0(3c)	3.0(3c)	3.0(3c)	3.0(3c)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(3e)	3.0(3e)	3.0(3e)	3.0(3e)	3.0(4a)	3.0(4d)
	MLOM	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3f)
C2960XR-48TD-I (Management)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5

HW	SW	5.7	5.8	6.0	6.1	6.2	6.3
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

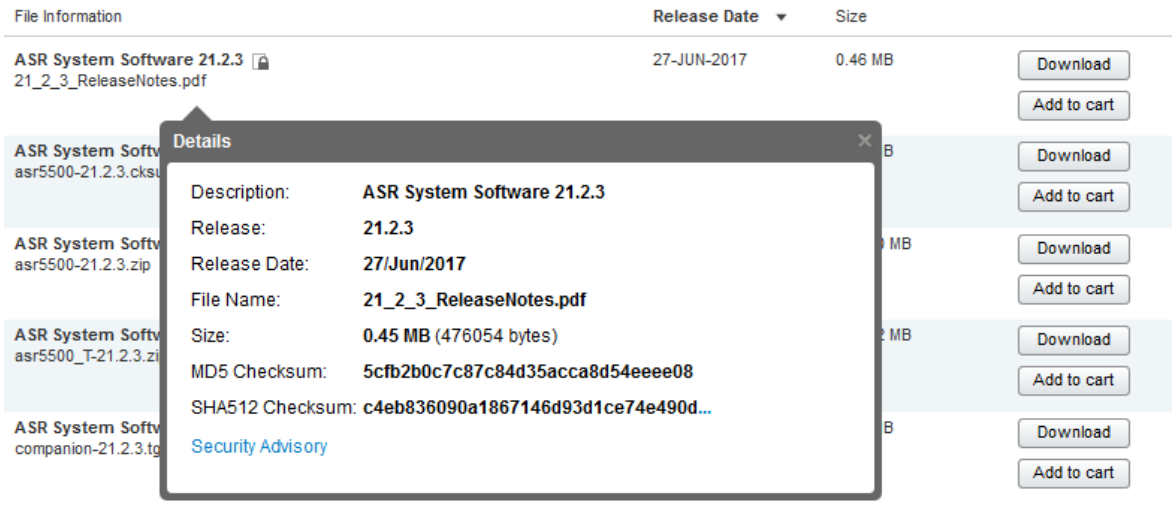
Firmware Updates

There are no firmware updates required for this release.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through Cisco.com Software Download Details. To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in Table 1 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the table below.

Table 1 - Checksum Calculations per Operating System

Operating System	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command > certutil.exe -hashfile *<filename>.<extension>* SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 *<filename>.<extension>*

Linux	Open a terminal window and type the following command
	
	$ sha512sum *<filename>.<extension>*
	
	Or
	
	$ shasum -a 512 *<filename>.<extension>*

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

StarOS software images are signed via x509 certificates. USP ISO images are signed with a GPG key. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

NOTE: Image signing is not currently supported for VPC-SI and/or VPC-DI software packages.

Open Bugs in this Release

The following table highlights the known bugs that were found in, and remain open in this software release.

NOTE: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Product Found*
CSCvk13391	[BP-CUPS] Sessmgr in over state with dedicated bearer	cups-cp
CSCvk17716	[BP-CUPS] On UBRes failure for Dynamic rule modification URRs getting removed for default Bearer	cups-cp
CSCvk42558	[BP-CUPS-VPP] Facility sessctrl restart: sn_msg_call_internal()	cups-cp

Bug ID	Headline	Product Found*
CSCvj90659	[BP-CUPS]sponsorIdentity parameter not populated in GTPP Custom35 CDR.	cups-cp
CSCvj93186	BP-CUPS: AFCID not seen in CDR for custom35 dictionary	cups-cp
CSCvk54440	StarOS 21.9 release does not contain the unittest for the traps with ifIndexes from 1357 to 1360	cups-cp
CSCvi53376	[BP-CUPS]: Session Manager reload at smgr_uplane_config_rule_options on Cisco PGW	cups-up
CSCvk21427	[BP-CUPS-VPP] Seg Fault at sessmgr_up_fapi_handle_stats_update()	cups-up
CSCvk27851	[BP-CUPS-VPP]: sxdemux process restarts every 6 mins	cups-up
CSCvk29167	[PLT-CUPS-VPP]: vpp stops on UP with 24 sessmgr	cups-up
CSCvk39591	[BP-CUPS-VPP] Segmentation fault at uplane_reset_saved_pdr_match_info on VPP Testbed	cups-up
CSCvj76251	[PLT-CUPS-VPP]: vpp_main in 'over' state with single subscriber 8Mbps data	cups-up
CSCvj77802	[BP-CUPS]: show subscriber data-rate not showing correct values	cups-up
CSCvj90571	[BP-CUPS] USAGE REPORT not sent in SxModResp even if QUERY URR is received in SxModReq	cups-up
CSCvk01813	[PLT-CUPS-VPP] Erroneous values in Analyzer statistics on load conditions.	cups-up
CSCvk01916	[BP-CUPS-VPP]Streams remain for infinite time even though no flows are there in a system.	cups-up
CSCvk05490	[PLT-CUPS-VPP]: [sessmgr 0 error] Timeout Processing: Time out, MSG ID: 8790, wheel Slot Id: 68	cups-up
CSCvk33357	[PLT-CUPS-VPP]: Can't make more than 50K calls at 40 attaches/sec	cups-up
CSCvk35955	[BP-CUPS-VPP] TEP row is not getting removed on call clear for collapsed call.	cups-up
CSCvk36699	[PLT-CUPS-VPP]: Analyzer statistics are corrupted	cups-up
CSCvk40097	[BP-CUPS]: Sessmgr restarted with sn_slist_remove_by_key	cups-up
CSCvj93176	BP-CUPS: packetCount is not incremented for R10 ULI change or Qos change	cups-up
CSCvk13327	SRP service not working when traffic is routed via two default route, 2nd default not reachable	pdn-gw
CSCvk34087	NAT IPs lost after session recovery when port-chunk-size is configured with higher values	pdn-gw
CSCvk05521	21.9_69629_5GNSA: Activate DCNR counters incrementing for Non-5GNSA PDP contexts	sgsn
CSCvk54113	Assertion failure at sess/sgsn/sgsn-app/gtp_c/gtapp_enc_ie	sgsn

Bug ID	Headline	Product Found*
CSCvk36855	Sessmgr Restart at access_get_nw_to_ms_gmm_stats_type	sgsn
CSCvk43563	Indirect Data tunnelling stats not updating after call is cleared on SGW.	sgw
CSCvk48646	Rmmgr restart on 21.9.CQ0.69887	staros
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros
CSCvj77813	show active-charging edr-udr-file statistics causing cli task restart	staros
CSCvk58670	[Cups] EM cluster not up	usp-uas
CSCvk60364	Deactivation failure due to timeout at AutoVNF	usp-uas
CSCvk56974	CUPS: Simultaneous undeployment for multiple vnfds leaves vnfd in Stopping state.	usp-usf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Resolved Bugs in this Release

The following table highlights the known bugs that are resolved in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Headline	Product Found*
CSCvj65113	[PLT-CUPS]: pool stats are not getting recovered post vpnmgr recovery	cups-cp
CSCvj65284	[BP-CUPS]:Assertion failure sgwdrv_ue_fsm_st_disconnecting_evt_snx_abortcall	cups-cp
CSCvk01188	[BP-CUPS]: S1/X2(with sgw change) handover to collapsed call not working for multipdn call	cups-cp
CSCvj99324	[BP-CUPS] Blocking Rf record generation on external triggers for CUPS calls	cups-cp
CSCvj74493	[PLT-CUPS-VPP] task restarts are seen while loading and deleting CUPs config on v21.x.Dx build	cups-up
CSCvj88126	[PLT-CUPS-VPP]: http Uplink data not working with a PureP fastpath enabled	cups-up
CSCvj88620	[PLT-CUPS-VPP]: VPP crash results in back to back npumgr crashes upon startup	cups-up
CSCvj90021	[PLT-CUPS-VPP] VPP offloading issue Flow mismatch on downlink side	cups-up
CSCvj98129	[PLT-CUPS-VPP]: VPPMOB lockup after 1-2 hours of call model run	cups-up

Bug ID	Headline	Product Found*
CSCvj99507	[PLT-CUPS-VPP] associate fast-path service cli taking longer time to get configured	cups-up
CSCvk00922	[PLT-CUPS-VPP]: VPP restarts with 1k calls at 500Mbps throughput	cups-up
CSCvk04792	[PLT-CUPS-VPP]: VPP dies when ports are binded	cups-up
CSCvj33257	[BP-CUPS]: Assertion failure at sx_tun_fsm_handle_sess_mod_req_msg	cups-up
CSCvj89071	[BP-CUPS]: Sxdemux reload observed in ipv6 service flow installation retry	cups-up
CSCvk03092	[BP-CUPS-VPP] Config deletion for nexthop	cups-up
CSCvj62438	Unexpected restart of ipsecmgr processes in ipmapi_notify_event_complete	epdg
CSCvi70010	Unexpected CDRs under Servers-Unreachable state for Volume Threshold	ggsn
CSCvi84457	Sessmgr restart when executing SGSN only commands on GGSN node	ggsn
CSCvi88688	sessmgr - Fatal Signal 11: Segmentation fault at sessmgr_ipv4_process_inet_pkt_part3_drop_packet()	ipsg
CSCvk01170	PGW reject change notification with unknown IMSI if its arrive 2.5 sec after GGSN/PGW handoff	pdn-gw
CSCvi47494	Cisco PGW seen with increasing GTPP Charging Purged counter	pdn-gw
CSCvj69251	[BP-CUPS]-Downlink data is not flowing when Pure P to Collapsed HO occurs with DSCP enabled	pdn-gw
CSCvj87548	[PLT-CUPS]: BFD is flapping every 5 mins on CUPS UP SAEGW context	pdn-gw
CSCvk09447	Change Notification reject_Invalid Message format: Message Received from incorrect peer	pdn-gw
CSCvh99909	Additional symbol added in HTTP header (quotation mark)	pdn-gw
CSCvj61992	Cisco PGW is seen not archiving CDR resulting in CDR loss	pdn-gw
CSCve61323	Flow ID sync with facility 86000 errror log messages	pdn-gw
CSCvj91954	Sessmgr restart seen at Cisco SAEGw in Supend Resume procedure	sae-gw
CSCvh67980	Sessmgr restart Assertion failure at sess/smgr/sessmgr_sgsn at sessmgr_sgsn_handle_modify_sess()	sgsn
CSCvh99115	Sessmgr restart at Cisco SGW when issued a drop event	sgw
CSCvj76682	sm restarts with Segmentation fault af snx_pgw_driver_recreate_pdn	sgw
CSCvi50398	core file size limited to 2048 bytes in VPC resulting in core file transfer failure	staros
CSCvj16336	Cli process restarting while running list mode all	staros

Bug ID	Headline	Product Found*
CSCvk05874	SITMAIN process assert leads to MIO Switchover when running update module p2p	staros
CSCvi76736	VRF config ip discard packet-when-no-route-in-vrf not being saved	staros
CSCvj28181	during boot storage-limit value was rejected, when system finish the boot then value can be applied	staros
CSCvj28849	OPENSSH Vulnerability - CVE-2016-8858	staros
CSCvj19974	Confdmgr: hitting artificial limit processing bukstats operational data message	staros
CSCvj85201	ultram-health uas report Authentication failed	usp-uas
CSCvj04691	AutoVNF recovery post upgrade does not spawn the upgraded image	usp-uas
CSCvj04799	AutoVNF upgrade failure - rollback to secondary image does not happen	usp-uas
CSCvi59139	iftask in over state with FDs alloc=800 used=976	usp-usf
* Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

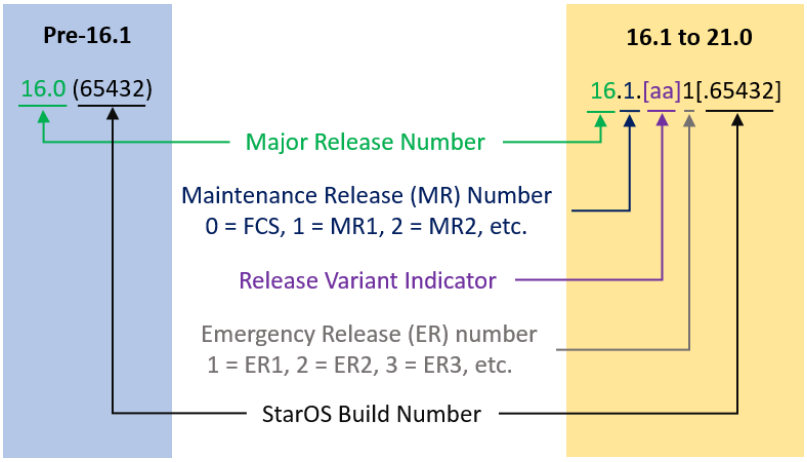
StarOS Version Numbering System

The output of the show version command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

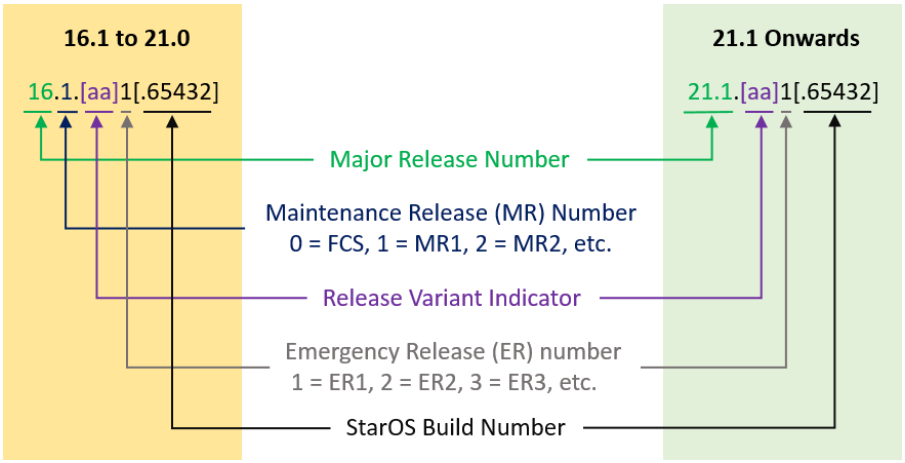
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the show version command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, show version will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".



The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".



In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 2 provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Package	Description
ASR 5500	
asr5500-<release>.bin	A zip file containing the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.bin	A zip file containing the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI	
qvpc-di-<release>.bin	The VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di_T-<release>.bin	The trusted VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di-<release>.iso	The VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di_T-<release>.iso	The trusted VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di-template-vmware-<release>.tgz	The VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvpc-di-template-vmware_T-<release>.tgz	The trusted VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvpc-di-<release>.qcow2.tgz	The VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-di_T-<release>.qcow2.tgz	The trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
VPC-SI	

Package	Description
qvpc-si-<release>.bin	The VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si_T-<release>.bin	The trusted VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso	The VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si_T-<release>.iso	The trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template-vmware-<release>.ova	The VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-<release>.ova	The trusted VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-<release>.qcow2.gz	The VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-si_T-<release>.qcow2.gz	The trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
StarOS Companion Package	
companion-<release>.tgz	An archive containing numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants.
Ultra Service Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles). Refer to Table 3 for descriptions of the specific bundles.
usp_T-<version>.iso	The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 3 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar	This package contains information and utilities for verifying USP RPM integrity.

Table 3 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.
usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.
* These bundles are also distributed separately from the ISO.	

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)