Release Notes for StarOS™ Software Version 21.6.0 and Ultra Service Platform Version N6.0

First Published: January 25, 2018
Last Updated: February 15, 2018

Introduction

These Release Notes identify changes and issues related to this software release. This release is the next major feature release since 21.5/N5.8.

Release Package Version Information

Software Packages	Version
StarOS packages	21.6, build 68695
Ultra Service Platform ISO	6_0_0-3006
usp-em-bundle*	6.0.0, Epoch 1587
usp-ugp-bundle*	21.6 0, build 68695, Epoch 1618
usp-yang-bundle	1.0.0, Epoch 1601
usp-uas-bundle	6.0.0, Epoch 1621
usp-auto-it-bundle	5.8.0, Epoch 1619
usp-vnfm-bundle	3.1.0.145, Epoch 1601
ultram-manager RPM*	1.1.0, Epoch 655
USP RPM Verification Utilities	6.0.0
* 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 UltraM 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
	StarOS	68173	68415	21.6.0, Build 68695
	ESC	3.1.0.116	3.1.0.116	3.1.0.145
	RH Kernel	7.3	7.3	7.3
	OSP	10	10	10
UCS C240 M4S SFF (NFVI)	BIOS	3.0(3c)	3.0(3c)	3.0(3c)
	CIMC (BMC)	3.0(3e)	3.0(3e)	3.0(3e)
	MLOM	4.1(3a)	4.1(3a)	4.1(3a)
C2960XR-48TD-I (Management)	Boot Loader	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
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E
	BIOS	7.59	7.59	7.59

HW	SW	5.7	5.8	6.0
Nexus 93180-YC-EX (Leafs)	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I5(2)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I5(2)	7.0(3)I5(2)

Firmware Updates

This software release includes a firmware upgrade for the Board Control FPGA (BCF) on the ASR 5500 MIO card.

- Previous BCF version: 4.1.0
- New BCF version: 4.8.0

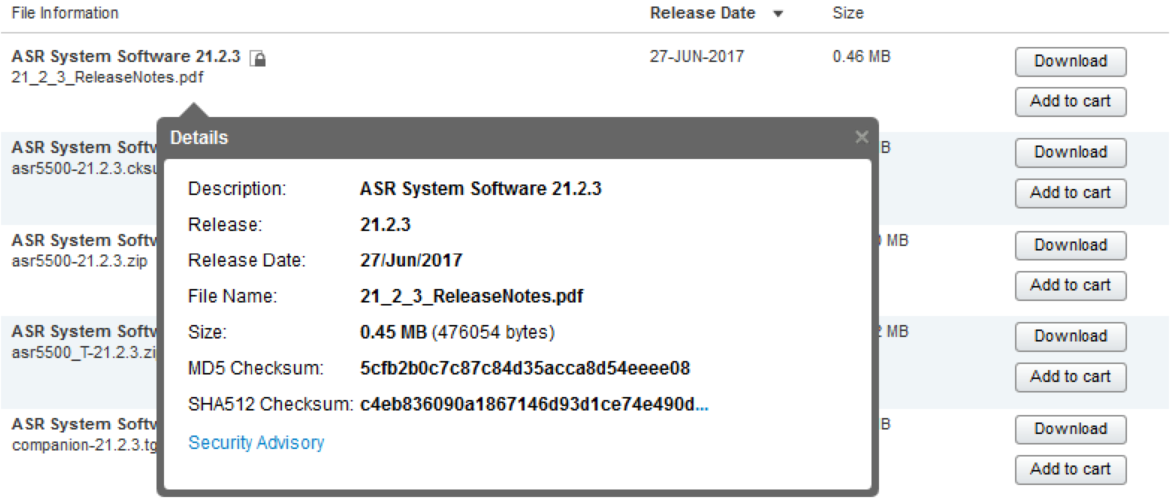
The new BCF firmware version provides:

- A 60 second lockout upon lowering the ejector sub-handle (interlock). Failures were observed in the field where an MIO that was being removed attempted to become Active as it was being removed. The remaining MIO would then go Standby causing a chassis failure. Now after the front panel ejector subhandle (interlock) is moved to the down position, the MIO is locked out for a period of 60 seconds and cannot become Active from the Standby state.
- A MIO reset and power down sequence when a BCF firmware upgrade is requested. A field failure was observed when an MIO with a lower revision of BCF firmware was installed in a chassis. The process of upgrading this BCF firmware on the new MIO caused inconsistencies on the chassis fabric signals which lead to other cards being reset. Upon receiving a request to reload the BCF firmware image from a newly programmed PROM, the BCF now first triggers a reset of all devices on the MIO card. After a short period of time the BCF powers the MIO card down for several seconds before the request to reload from PROM is performed.
- Improved the use of MIO presence pins to reduce the chance of incorrect Active state changes. This change affected the use of both the MIOs presence pins. Additionally, a signal filter was added to both MIOs presence pins to prevent false MIO state changes, such as during removal of inserts.

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.



File Information	Release Date	Size
ASR System Software 21.2.3 21_2_3_ReleaseNotes.pdf	27-JUN-2017	0.46 MB
ASR System Softw asr5500-21.2.3.cksu		B
ASR System Softw asr5500-21.2.3.zip		MB
ASR System Softw asr5500_T-21.2.3.zi		MB
ASR System Softw companion-21.2.3.tg		B

Details

Description: ASR System Software 21.2.3
Release: 21.2.3
Release Date: 27/Jun/2017
File Name: 21_2_3_ReleaseNotes.pdf
Size: 0.45 MB (476054 bytes)
MD5 Checksum: 5cfb2b0c7c87c84d35acca8d54eeee08
SHA512 Checksum: c4eb836090a1867146d93d1ce74e490d...
Security Advisory

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 for This Release

The table below 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*
CSCvh59780	Sessmgr restart in egtpc event handler path	mme
CSCvg36262	Split the current MME-Decor related stats for TAU and Attach procedures	mme
CSCvg95957	Single instance of Bulkstat facility restart seen on active CISCO ASR5500	pdn-gw
CSCvh24483	sessmgr crashes when tcp proxy-mode is enabled with high data throughput	pdn-gw
CSCvh67681	20% SM CPU increase when Traffic Optim is enabled with 100% heavy session in single event perf test	pdn-gw
CSCvh64982	Planned SRP switchover followed by switchover due to BGP failure - aaamgr restarts	sae-gw
CSCvh69926	Session manager restart at imsa_dpca_clear_outstanding_trans_by_transid	sae-gw
CSCvh54162	[ePDG] performing iftask restart is causing SF to restart on ultraM with servicemode as epdg	staros
CSCvh68111	The beakerd process has a memory leak	staros
CSCvh66730	iftask complaing "mbuf_usage_debug_info:877 Invalid mempool" with large # of thread	staros
CSCvd91619	Element Manager - Suspend/Resume not working after CF Switchover	usp-usf

* Information in the “Product Found” column identifies the product in which the bug was initially identified.

Resolved Bugs for This Release

The table below 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*
CSCvg70907	Session manager reload observed at EPDG Egress during handling GTP message.	epdg
CSCvg76203	ipsecmgr restats at ipsecmgr_make_app_state_cb	epdg
CSCvh07852	Sessmgr task restart due to same call-id being reused by sessmgr	epdg
CSCvg30872	For Cisco GGSN "dns-client context" is not configured by default and doesn't work	ggsn
CSCvh01103	Bad UDP checksum error when Header Enrichment is applied for MMS over WSP	ggsn
CSCve35811	Session Manager restarts on failed assert in sn_gt_encode_pdp_context_ie	mme
CSCvf74768	Ghost enodeB associations	mme
CSCvf94319	sessmgr restart at libc.so.6/__memcpy_ssse3_rep()	mme
CSCvg27273	Two MMEMGR tasks not re-created after PSC card migration	mme
CSCvh29852	mme not sending cs-fallback-indicator in initial context setup request (mt-access paging)	mme
CSCvc95583	Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c	pdn-gw
CSCvd54827	IPv6 over L2TP behaviour with Access-Control-List	pdn-gw
CSCve45216	Prefix delegation routing issue	pdn-gw
CSCvg03658	PGW sends IPV6 DNS addr in CS Resp in S2b from context when not configured in APN	pdn-gw
CSCvg10694	CLI Process task restart while trying to display PGWCDRs in show logs	pdn-gw
CSCvg36977	aaamgr and sessmgr in over state after back-to-back double fault scenario.	pdn-gw
CSCvg49509	Header Insertion fails with FAPA config enabled	pdn-gw
CSCvg63020	Traffic stops matching to group of ruledefs	pdn-gw
CSCvg70586	Software issue related to ACS manager functionality	pdn-gw
CSCvg70738	tcp check-window-size CLI default value changed after upgrade	pdn-gw
CSCvg73268	Rule Matching stops working for ruldefs which contains p2p sub proto in upgrade scenarios	pdn-gw
CSCvg78431	Session manager restart while rating the HTTP URL	pdn-gw
CSCvg81684	Session manager restart in EDR generation path	pdn-gw

Bug ID	Headline	Product Found*
CSCvg89252	aaamgr restarted multiple times on srp switch-over	pdn-gw
CSCvh01829	Unexpected memory allocation for sessmgrs	pdn-gw
CSCvh04102	CCR-U not including AN-GW-ADDRESS with configuration "diameter encode-event-avps always"	pdn-gw
CSCvh12556	SessMGR reboots after SRP swithover if APN is removed on the standby before the SRP switchover	pdn-gw
CSCvh13140	Stats at the PGW level are incorrect.	pdn-gw
CSCvh13882	Facebook ruldef hit after removal from rulebase	pdn-gw
CSCvh14879	ECS increments the SEQ number twice in the uplink direction	pdn-gw
CSCvh21425	Charging-Action with terminate-flow allows traffic to pass	pdn-gw
CSCvh29929	Sessmgr restart observed during PGW to GGSN handover	pdn-gw
CSCvg58040	Sessmgr restarts on saegwdrv handling.	sae-gw
CSCvg77087	XL - GGSN/SAE-GW on VPC-DI - aaamgr in Active CF card in Memory warn state	sae-gw
CSCvg79504	Sessmgr restart after CLI <b>task kill facility hamgr instance</b> is executed on standby chassis	sae-gw
CSCvh16674	APN-AMBR not be sent if LI trigger is enabled over already Active call.	sae-gw
CSCvh27968	SM reload observed during 3g to LTE HO for SAEGW NEMO Call when uplink pkt received on new tunnel	sae-gw
CSCvg26420	Sessmgr restarts after segfault @ function mrme_aaa_handle_acct_stop_as_server()	samog
CSCvg92118	samog wrongly rejects UBR with syntactic error	samog
CSCve75767	Printout discrepancy regarding DPC Congested/Available state.	sgsn
CSCvf48725	SGSN is releasing PDP after receiving an Update PDP Response from Roamer GGSN.	sgsn
CSCvg74239	Incorrect encoding of mnc values in rnc-fqdn dns query when the encoding is hexadecimal	sgsn
CSCvg95945	SGSN send CPC with wrong IMEI	sgsn
CSCvg40100	[UltraM-FOA][TMO] Both CFs reboot when di net ports on any one CF goes down	staros
CSCvg64284	Threshold process goes into warn state because of memory.	staros
CSCvg76217	configuration checksum calculation is higher than internal allowed limit	staros
CSCvg80533	Possible memory leaks on error paths for radius and radius group schema	staros
CSCvg85379	VPC-DI chassis initialization permanently stalled by emctrl	staros

Bug ID	Headline	Product Found*
CSCvh11052	After reload, header encryption is lost	staros
CSCvh32798	Threshold process goes into warn state because of memory.	staros
CSCvh50428	Gy Validity timeout is being reported as "ServiceConditionChange:PDP context release" in CDR's	staros
CSCvh60072	The beaker task is in over state	staros
CSCvg58573	Deployment fails do to "Failed to get deployment data" error on consecutive activation/deactivation	usp-uas
CSCvg55135	Auto-stager substituting os_username for the project id when trying to create a deployment	usp-uas
CSCve72573	Audeploy/autoit/autovnf has no name in log file name of log collector whereas esc does have	usp-uas
CSCvf31799	Assert Failure at usp_confdmgr_register_message() upon upgrade	usp-usf
* Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

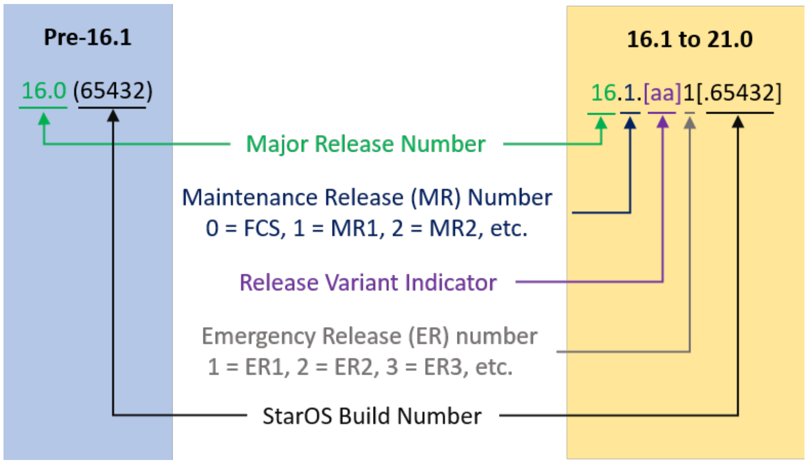
StarOS Version Numbering System

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.

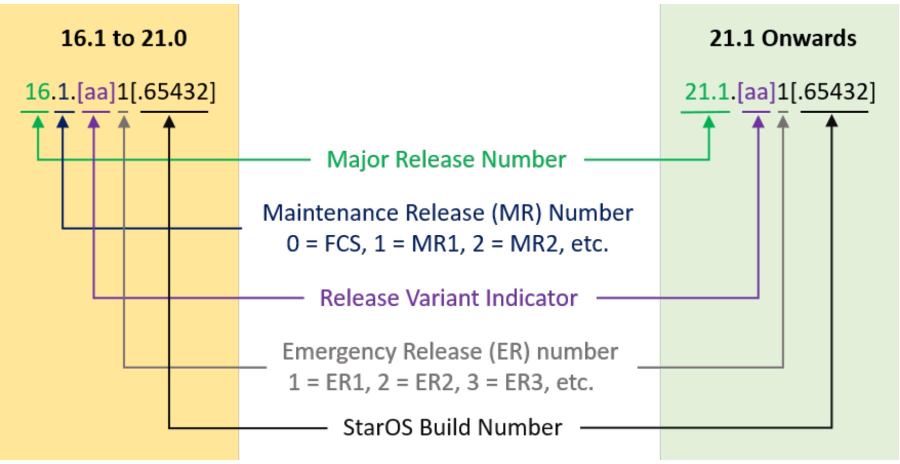
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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


Pre-16.1
16.0 (65432)
16.1 to 21.0
16.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

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


16.1 to 21.0
16.1.[aa]1[.65432]
21.1 Onwards
21.1.[aa]1[.65432]
Major Release Number
Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.
Release Variant Indicator
Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.
StarOS Build Number

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 lists 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.

Package	Description
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	
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.

Package	Description
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)