Release Notes for StarOS™ Software Version 21.10.0 and Ultra Service Platform Version 6.4

First Published: November 2, 2018
Last Updated: November 5, 2018

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.9/N6.3.

Release Package Version Information

Software Packages	Version
StarOS packages	21.10, build 70597
Ultra Service Platform ISO	6_4_0-6803
usp-em-bundle*	6.4.0, Epoch 4876
usp-ugp-bundle*	21.10 0, build 70597, Epoch 4815
usp-yang-bundle	1.0.0, Epoch 4661
usp-uas-bundle	6.4.0, Epoch 4879
usp-auto-it-bundle	5.8.0, Epoch 4869
usp-vnfm-bundle	4.3.0.121, Epoch 4662
ultram-manager RPM*	2.2.0, Epoch 292
USP RPM Verification Utilities	6.4.0
* 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	5.8	6.0	6.1	6.2	6.3	6.4
	StarOS	68415	21.6.0, Build 68695	21.7.0, Build 68897	21.8.0, Build 69296	21.9.0, Build 69977	21.10.0, Build 70597
	ESC	3.1.0.116	3.1.0.145	3.1.0.145	4.0.0.104	4.2.0.74	4.3.0.121
	RH Kernel	7.3	7.3	7.3	7.4	7.5	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(4a)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(3e)	3.0(3e)	3.0(3e)	3.0(4a)	3.0(4d)	3.0(4d)
	MLOM	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3f)	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
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)I7(3)	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)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

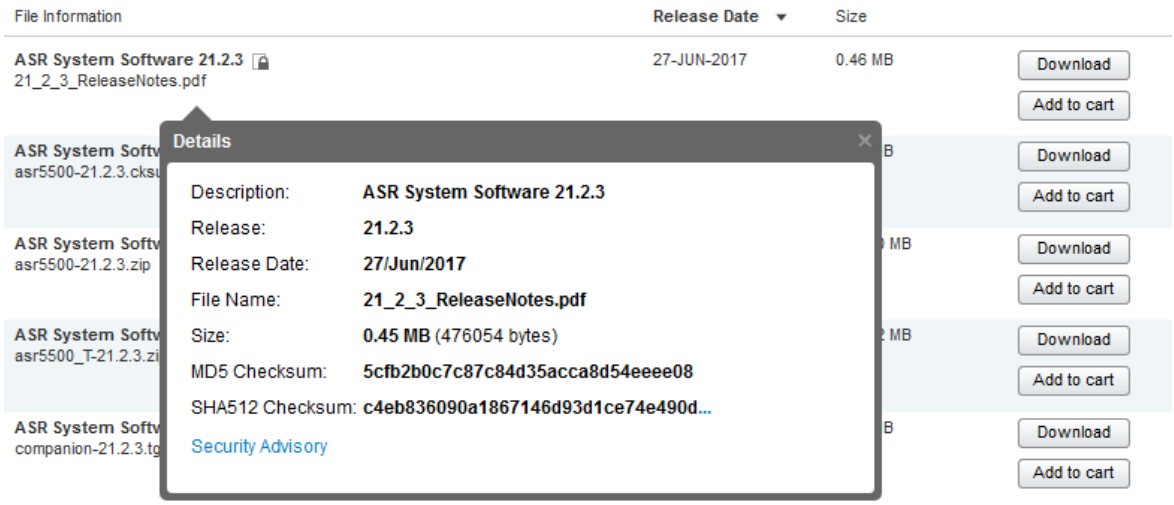
Firmware Updates

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, see the following table.

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 lists 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*
CSCvk52151	[BP-CUPS]: Huge session disconnect with reason sx-cntxt-not-found	cups-cp
CSCvm48160	[PLT-CUPS] chmgr restart unhandled sn_event_file's in migrating proclet chmgr	cups-cp
CSCvi53376	[BP-CUPS]: Session Manager reload at smgr_uplane_config_rule_options on Cisco PGW	cups-up
CSCvk52159	[BP-CUPS]: huge session disconnect with reason sx-mand-ie-incorrect	cups-up
CSCvk56280	[BP-CUPS-VPP]: sessmgr restart at uplane_policing_charging	cups-up
CSCvk62265	[BP-CUPS]: UP never re-initiate SX association if it comes back before SX faillure detected in UP	cups-up
CSCvk66464	[BP-CUPS]: Sessmgr reload at smgr_match_dyn_rule_filter	cups-up
CSCvm54234	[PLT-CUPS-VPP] Call is getting dropped after performing shutdown-noshutdown-shutdown interface	cups-up
CSCvk46857	[PLT-CUPS-VPP]: vpnmgr restart while removing crp config	cups-up
CSCvm47437	[BP-ICUPS]:Analyser/RB statistics are not counting DL dropped offloaded packets.	cups-up
CSCvm56058	[BP-ICUPS]: Streams created with state PASSIVE and packets pass through slow path.	cups-up
CSCvm56190	[BP-ICUPS]: packets sent through slow path after PDN-UPDATE.	cups-up
CSCvm57966	[BP-ICUPS] First DL pkt of UDP flow creating stream in passive state instead of active state	cups-up
CSCvm72250	[PLT-CUPS-ICUPS] sessmgr and vpp crashes and DPC2 cards in Offline state on 21.10.M0.70328	cups-up
CSCvm50353	[BP-ICUPS] : SGW sends TEP entry Updation with IPV6 remote and local address during HO	pdn-gw
CSCvm55782	[BP-ICUPS]:Dynamic Rule flow status change from Discard to Allow All is not working	pdn-gw
CSCvm63590	[PLT-ICUPS-VPP]: Update to DCCA triggered 1 pkt later then expected.	pdn-gw
CSCvm79365	[BP-ICUPS]: Data over new dedicated bearer after gngp-collapsed HO sent through slow path.	pdn-gw
CSCvm91229	[BP-ICUPS] : sessmgr restart at fapi_tp_process_incoming_local_row_req() sp=0xffccd588()	pdn-gw
CSCvm75776	[BP-ICUPS]:Policer table is deleted,created twice on Dynamic Rule deletion, bearer movement for GBR	pdn-gw
CSCvm83968	[CUSP] need to handle interworking of URL-readdressing and CUSP feature.	pdn-gw
CSCvn03518	Idle timer expires 10 seconds earlier than it ideally should when data sent.	pdn-gw
CSCvn13800	sessmgr restart at function dh_api_delete_handle	pdn-gw
CSCvm82008	[BP-ICUPS]:HTTP volume based offload is not happening after PDN update	sae-gw

Bug ID	Headline	Product Found*
CSCvn09483	21.10_70287_SGSN: Subscriber IMEI check frequency config not working properly during InterSRAU event	sgsn
CSCvm93185	[SGSN] DNS Naptr weight based load balancing not taking place	sgsn
CSCvm45981	[PLT-ICUPS]:TCP & UDP Packets drop observed at VPP for Single PGW at 500+ Mbps with 5 & 2 flows	staros
CSCvk60364	Deactivation failure due to timeout at AutoVNF	usp-uas
CSCvm91778	AutoVNF NETCONF trace has passwords in the clear	usp-uas
CSCvm03898	VnfDiags not working correctly	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 lists 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*
CSCvj77515	[BP-CUPS]: sessmgr restart when attempting an SAEGW Gx call on CUPS setup	cups-cp
CSCvk13379	[BP-CUPS]Sessmgr reload is observed on PGW Control Plane while sending Sx Session Reporting Request	cups-cp
CSCvk48006	[BP-CUPS]: Behaviour on Sx PFD messages timeout - UP stuck in Not configured state	cups-cp
CSCvk56822	[BP-CUPS]:Sx Path failure causing call drop after srp switch-over	cups-cp
CSCvk54440	StarOS 21.9 release does not contain the unittest for the traps with ifIndexes from 1357 to 1360	cups-cp
CSCvk21427	[BP-CUPS-VPP] Seg Fault at sessmgr_up_fapi_handle_stats_update()	cups-up
CSCvk47500	[BP-CUPS-VPP] RS packet handling is incorrect in VPP fastpath.	cups-up
CSCvk58383	[BP-CUPS-VPP] Assertion failure at Function: sxmgr_process_session_establish_req	cups-up
CSCvk62132	[PLT-CUPS-VPP] IP fragmented packets are dropped by VPP	cups-up
CSCvk65470	[BP-CUPS] sessmgr resrart libc.so.6/__strlen_sse2_bsf()	cups-up
CSCvm06471	[BP-CUPS-VPP] Sessmgr reload at uplane_reset_saved_pdr_match_info	cups-up
CSCvm08142	[BP-CUPS]:Sessmgr reload at uplane_http_accel_check.isra.116	cups-up
CSCvm08681	[BP-CUPS]: sessmgr reload at set_stream_operations	cups-up
CSCvj76251	[PLT-CUPS-VPP]: vpp_main in 'over' state with single subscriber 8Mbps data	cups-up
CSCvj81306	[BP-CUPS]: [sessmgr 12341 error] [SXAB] Update PDR not found with PDR ID 0x7	cups-up
CSCvk39031	[BP-CUPS-VPP] TOS not getting applied on d/l inner packet from qci qos mapping table.	cups-up

Bug ID	Headline	Product Found*
CSCvk40097	[BP-CUPS]: Sessmgr restarted with sn_slist_remove_by_key	cups-up
CSCvk42806	[BP-CUPS-VPP] Drop stream is not getting onloaded on installing high priority rule.	cups-up
CSCvk51032	[BP-CUPS-VPP] sessmgr crash(seg fault)sx_tun_fsm_handle_sess_mod_rsp_evt	cups-up
CSCvk54274	[BP-CUPS]: UP is crashing and call in not coming up when subs-class with rulebase config is present	cups-up
CSCvk55699	[BP-CUPS]: Issues with un-optimized rules in GoR. Traffic always matches Un-optimised rules in GOR	cups-up
CSCvk56186	[PLT-CUPS-VPP] LC row is not removed on removal of URR.	cups-up
CSCvk56305	Sessmgr restart seen when the link btw CP and UP are broken for some reason	cups-up
CSCvk56703	[PLT-CUPS-VPP]: 200k scaling test vpp restart memif_interface_tx ()	cups-up
CSCvk58697	[BP-CUPS-VPP] US37480: Support correct charging of packets which do not go for RuleMatch	cups-up
CSCvk64528	[BP-CUPS-VPP]: user-plane rule base statistics packet count swapped	cups-up
CSCvm00476	[BP-CUPS] sxdemux facility in over state	cups-up
CSCvm09336	[BP-CUPS] "show subscribers user-plane-only" discrepancy with active flow output	cups-up
CSCvm20512	[BP-CUPS-VPP] sessmgr restart on rulebase change from egcdr disable to enable.	cups-up
CSCvm36773	[PLT-ICUPS-VPP] Stream Operations not working after stream-modify	cups-up
CSCvm46282	[BP-ICUPS-VPP]L3 L4 actions not applied on UL streams for pipelined GET	cups-up
CSCvm47423	[BP-ICUPS] : CA level TOS marking is not getting applied for HTTP onloaded response packets	cups-up
CSCvm55905	[BP-ICUPS]: packets sent through slow path after HO.	cups-up
CSCvm66988	[BP-ICUPS]:HTTP volume based offload not working correctly	cups-up
CSCvm47411	[BP-ICUPS] Total Accel Pkts counter is not incremented in under FTP Analyzer statistics	cups-up
CSCvm51442	[GGSN/PGW] Right PDP failure cause for supported IPv6 should be "Unknown PDP address or PDP type"	ggsn
CSCvk68643	Ruledef with imsi pool configuration not getting matched appropriately	ipsg
CSCvm77890	[BP-ICUPS]: UDP UL/DL pkts are dropping for dedicated bearer(GBR bearer).	pdn-gw
CSCvj09057	PGW detect wrong RAI change event trigger when ULI change from CGI+RAI to CGI	pdn-gw
CSCvk27330	PGW retransmits Gy CCR-U without previous USU AVP in case of RAR-CCR collision	pdn-gw
CSCvk29371	gtpc peer-salvation keyword is missing under context level configuration	pdn-gw
CSCvk43057	Sessmgr restart seen at PGW while adding frame route received from radius.	pdn-gw
CSCvk59689	PGW: CCR sent with wrong Destination Realm after Gx recovery	pdn-gw
CSCvk61018	[BP-ICUPS]:offloaded packets are counted double in active charging flows all output	pdn-gw

Bug ID	Headline	Product Found*
CSCvk65827	[BP-ICUPS] : Uplink data not reaching PDN side	pdn-gw
CSCvm03497	Multiple sessmgrs to go into warn state due to high memory at Cisco PGW	pdn-gw
CSCvm05227	[BP-ICUPS-] sessmgr restart on single pgw call when tried to increase throughput beyond 4Gb.	pdn-gw
CSCvm06442	[BP-ICUPS]: Garbage TIME-IDLE value in show sub all for downlink udp traffic	pdn-gw
CSCvm08447	[BP-ICUPS]:L4 TCP/UDP Bytes are not getting correctly updated in analyser stats	pdn-gw
CSCvm16264	[BP-ICUPS] fastpath_stream_add():sessmgr error logs (streams not created/no LCs updated)	pdn-gw
CSCvm33939	[BP-ICUPS-VPP]:Sessmgr restart at migrate_clnt_prepare_procl_for_migration() function	pdn-gw
CSCvm34028	[BP-ICUPS] : After Recovery, data packets through sessmgr	pdn-gw
CSCvm47811	Adding debug info to understand restart counter change from SGW causing PGW to mark sessions down	pdn-gw
CSCvm50715	[BP-ICUPS]:acsmgr_process_fp_flow_stats() casuses sessmgr restart	pdn-gw
CSCvm50721	[BP-ICUPS]:After AMBR change acs_handle_sess_event_notify() seen	pdn-gw
CSCvm55788	[BP-ICUPS]:sessmgr restart observed on collocated calls and with http traffic on TMO setup.	pdn-gw
CSCvm74718	[BP-ICUPS] : PC: [097a0248/X] is_acs_rule_dscp_enabled()	pdn-gw
CSCvm81755	[BP-ICUPS]: Bandwidth Policy Flow Id change after Rulebase change is not getting applied	pdn-gw
CSCvm83704	egtpinmgr restart when MIO switchover happened	pdn-gw
CSCvm83730	[BP-ICUPS] [ICSR] Crash in sessmgr_fp_recover_clp_abstract_data during ICSR	pdn-gw
CSCvm89565	[BP-ICUPS]: UDP downlink data is dropped on 70457	pdn-gw
CSCvn00082	Create Session Response with MSISDN PCO Option fails with consecutive 0's	pdn-gw
CSCvj35699	Session manager task restart observed while applying url-readdressing.	pdn-gw
CSCvk14784	Accelerated flows are not ITC BW-limited when BW-ID configured in charging-action.	pdn-gw
CSCvm36611	Cisco PGW Egtpmgr restart seen after CLI "show egtpc peers path-failure-history"	pdn-gw
CSCvm54632	Session manager on standby chassis is in memory over state.	pdn-gw
CSCvm83724	[BP-ICUPS]:Data is not offloaded after PDN update is done via dyn rule installation	sae-gw
CSCvm54230	Cause Source bit discrepancy within Create Bearer Response message on SPGW	sae-gw
CSCvm62241	ASR5500- Assertion failure at sess/smgr/sessmgr_pgw_li.c:450	sae-gw
CSCvj83211	SM fail due to Fatal Signal at <unknown>	sgsn
CSCvd89962	sessmgr Assertion Failure in egtpc_handle_user_sap_event()	sgsn

Bug ID	Headline	Product Found*
CSCvk47572	Duplicate messages over S13 interface.	sgsn
CSCvj49375	Session manager restart due to EGTPC Update bearer response event	sgsn
CSCvj81432	Periodic card shutdown observed on Standby CF card.	staros
CSCvf65641	Consecutive EGTPCPathFailClear SNMP traps without EGTPCPathFailSet	staros
CSCvm73155	Unable to update module p2p after unplanned DPC migration	staros
CSCvi12895	FloatingIP assignment should be unique across VMs of VNFs	usp-uas
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
CSCvk60364	Deactivation failure due to timeout at AutoVNF	usp-uas
CSCvk56974	CUPS: Simultaneous undeployment for multiple vnfds leaves vnfd in Stopping state.	usp-usf
CSCvm03898	VnfDiags not working correctly	usp-usf

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

Operator Notes

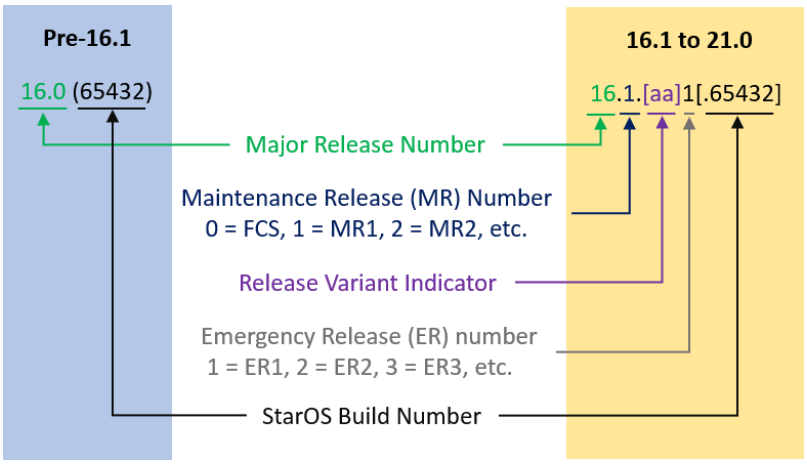
StarOS Version Numbering System

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.

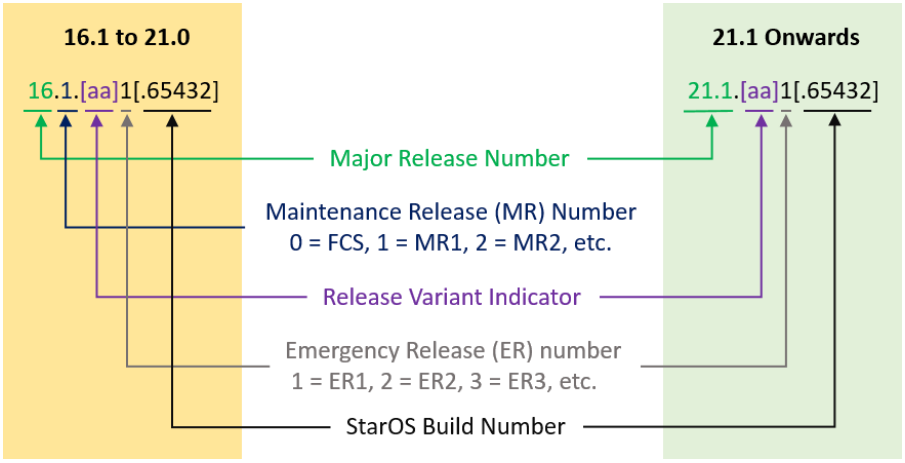
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

Package	Description
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.
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.

Package	Description
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)