Release Notes for StarOS™ Software Version 21.28.m12

First Published: September 03, 2023
Last Updated: September 03, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.28.m10. These release notes are applicable to StarOS and RCM products.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.28.m12, build 91080

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 the complete list of CUPS documentation available for this release, go to https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html.

For the complete list of the corresponding StarOS documentation, go to https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/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.

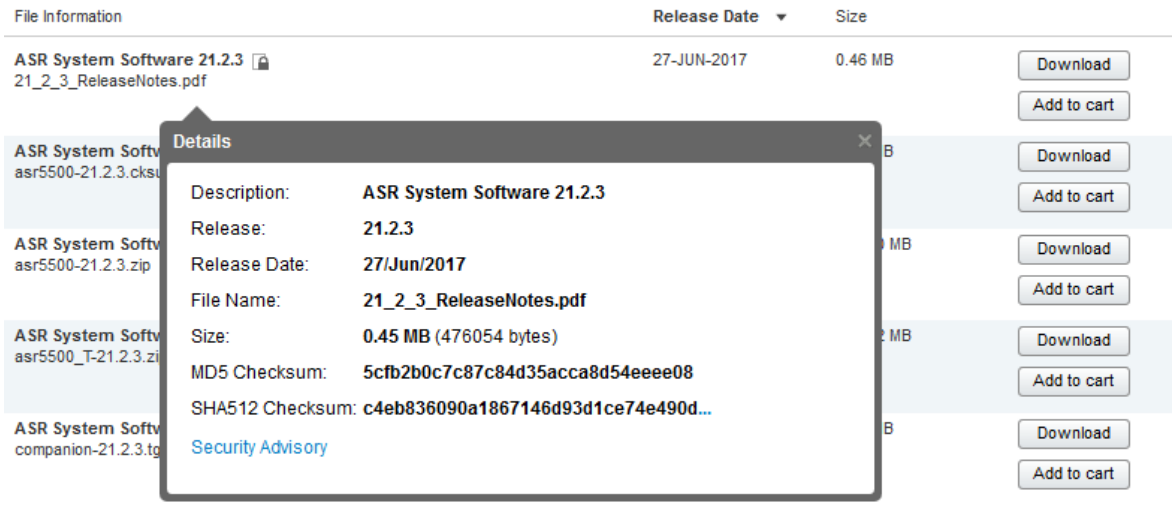
Firmware Updates

There are no firmware upgrades 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 2 and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop see Table 2.

Table 2 - 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

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs in this Release

The following table lists 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.

Table 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwh43087	[CUPS 21.28.m10] URR not created during re-installation of previously removed ruledef	cups-cp
CSCwh43745	Assertion failure at sess/egtp/egtpc/egtpc_interface.c:280	cups-cp
CSCwe86265	Behavior of command documentation in CUPS-CP User Guide	cups-cp
CSCwf26675	[BP-CUPS] Abnormal Release record closure for 3g call with custom38 dictionary	cups-cp
CSCwf51104	[LI] Wrong timestamp format on event delivery interface	cups-cp
CSCwf42495	[CUPS-CP] [LI] Third target interception for the same subscriber NOT working as expected	cups-cp
CSCwc29508	[BP-CUPS][sessmgr 12341 error][essmgr_uplane.c:36574][SXAB] UE IP Address is different in Traffic	cups-up
CSCwh43447	No IMS Signaling is received on LMISF side	cups-up
CSCvu76574	[BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error	cups-up
CSCwh03670	[CUPS-UP] Downlink total fp packets not shown correctly in case of http out of order packet	cups-up
CSCwh20389	EGTPUPathFail not generated in CP node	cups-up
CSCwh17135	Intermittent Mute call issue on 21.28.m10(90398)	cups-up
CSCwb83398	[BP-CUPS] Lots of error logs GTPU Recover Session Failed for GTP-u Peer on standby UP	cups-up
CSCwc73243	[BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721	cups-up
CSCwh01131	"Mon sub feature cases are not working for Pures, Purep and Collapsed call model"	cups-up
CSCwe73462	[BP-CUPS][sessmgr 10396 error]smgr_recovery.c:13989]Sessmgr-10Recover call from CRR failed post SR	cups-up
CSCwf13605	ipsecdemux crash on asr5500 during crypto call model longevity	epdg

Bug ID	Headline	Product Found*
CSCwf87704	StarOs add an un-expected gtpu-service	ggsn
CSCwh43672	correct the cause code from DUE_TO_SUSPENSION to UNABLE_TO_PAGE_UE	mme
CSCwf92141	[MME] SessMgr restart at mme_egptc_set_pdn_state.isra.283()	mme
CSCwh04501	mmemgr crash in mmemgr_rx_sctp_pdu_from_mmedemux() function	mme
CSCwc65963	sessmgr restart is seen when configuring and unconfiguring Lawful intercept CLIs multiple times	mme
CSCwd29108	[NSO-MOB-FP] error with nfv-vim package with NSO 5.7.6.2 or 5.8.4 or 5.6.8 and MFP 3.4	nso-mob-fp
CSCwh25258	[MFP] mobility-library used to upgrade p2p does not handle properly p2p with 4 sets of digits (w ER)	nso-mob-fp
CSCwf87596	"On qvpc, MPLS/VPN - Staros is reversing the bottom/top labels"	pdn-gw
CSCwh39018	Need CLI user guide support for new CLI as part of CSCwf90908	pdn-gw
CSCwc53741	Checkpointed information lost after checkpointmgr pod restart	rcm
CSCwe62325	Ubuntu 16.04 ESM/18.04LTS/20.04LTS/22.04LTS/22.10 : systemd vulnerability seen in RCM VM Nessus Scan	rcm
CSCwf75570	ApacheTomcat 9.0.71 <9.0.74 DoS and ApacheTomcat 9.0.0 > 9.0.75 vulnerabilities in 21.28.mx/x RCMVM	rcm
CSCwb74230	Switchover statistics info is missing in Switchover verbose statistics.	rcm
CSCwc10141	keepalived to controller notification fails but no retry	rcm
CSCwh41755	RCM is pushing negative config with one extra exit resulting UPFCfgPushError trap	rcm
CSCwd91543	IKE notify packets are not responded after pod reload	rcm
CSCwf93799	session manager Assertion failure at sess/snx/drivers/sgw/sgw_epsb_fsm.c	sgw
CSCwc67766	[UPF_SVI] N4 Session Report request is getting assigned wrong peer IP addr ::ffff:192.10.25.23	smf
CSCwd27711	[UPF-SVI] : Uplane received invalid far id in PDU	smf
CSCwf08000	[SVI-UPF] Error logs Remove PDR PDR with ID observed	smf
CSCwf98183	[UPF-ST] Continuous error logs on active RCM UPF “Active and Inactive RAT pdr CH validation failed”	smf
CSCwe74835	[SMF-MONSUB]CLI instance id should be same in START/STOP of Trace.	smf
CSCwf01246	[UPF-ST] : Sessmgr error logs “[N4] UE IP Address is different in PDR with PDR ID “	smf
CSCwf86536	[UPF-ST] : rx missed obsrerved in vpp show hardware interfaces discarding the flows	smi
CSCwd51484	Apache Tomcat 9.0.0-M1 Req Smuggling and Azul Zulu java (2022-10-18) Mulitple Vulnerabilities	smi
CSCwe79529	opscenter 2 container are crashing (confd & confd-notifications)	smi
CSCwd81548	[5GaaS] Edge proxy NFs rely on NF restarts to apply config changes	smi
CSCwe51959	v21.28.mx as the upstream branch :: RHEL-8 Build Issues fix in downstream Dev Branch v21.28.ZVx	staros
CSCwf26822	push config-to-up all takes longer than 5mins to finish	staros

Bug ID	Headline	Product Found*
CSCwf04131	[UPF-MONSUB]Extra Sx report for MONSUB report.	upf
CSCwf00180	[UPF-SVI] : Seen Error logs "[CDR 1966 - URR ID -2147435417]" with ICSR SW	upf
CSCwf62665	[UPF-MONSUB]:uplink data pkts going via slowpath are not captured in FP trace	upf
CSCwf96687	[UPF-ST] sm restart observed on stdby HUPF at sessmgr_recover_uplane_pdr_info() post sessmr recovery	upf
CSCwf08057	[UPF-SVI] : Seen Update FAR not found with FAR ID 0x11e with RCM planned/Unplanned SW	upf
CSCwf11828	[UPF-ST]: Error logs Invalid FAR with id 5 received in PDU. IMSI: 311480071230621 Interface: N4	upf
CSCwe80795	[UPF-MONSUB]GTPU end marker is not captured in slowpath pcap.	upf
CSCwh02919	[UPF-ST]: 4g converged and non converged calls getting drop with echo req/res on MPLS over N9	upf
CSCwd99519	[UPF-ST] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	upf
* 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 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.

Table 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwd33517	show apn statistics shows wrong value for GERAN and UTRAN users	cups-cp
CSCwh04674	INSUFFICIENT_BEARER_RESOURCES high	cups-cp
CSCwe86228	cli display shows contradictory information for UP-Group name and UP-NODE-ID	cups-cp
CSCwf86398	"After WLAN->LTE handover, CP is updating non-existing FAR, leading to handover failure."	cups-cp
CSCwh17010	Sessmgr task restarted at function "egtpc_handle_update_bearer_req_evt()"	cups-cp
CSCwh30213	sessmgr showing active callline count has reached to max allowed callline	cups-cp
CSCwf63318	(CUPS) SGW incorrectly handling collision between MBR & CBR during N26 handover	cups-cp
CSCwe94031	BP-CUPS] Assertion failure at sess/sx/sxc/sx_evt_handler_comm.c:625	cups-cp
CSCwd93230	"[CUPS UP] When dynamic rule precedence is zero, UP is not accounting packet in URR "	cups-up
CSCwc99110	[BP-CUPS]: Assertion failure at sess/smgr/sessmgr_gtpu.c sessmgr_egtpu_signalling_routine()	cups-up
CSCwe85093	UP core files generated after removing ruledefs	cups-up
CSCwh32137	[BP-CUPS] Outer header removal type[1] does not match the configure gtpu endpoint for PDR ID	cups-up
CSCwf75558	"show subscribers idle-time" displays the incorrect UE sessions	cups-up

Bug ID	Headline	Product Found*
CSCwh17326	[BP-CUPS]: Observed Assertion failure at func sessmgr_uplane_gtpu_tx_update on longevity setup	cups-up
CSCwf12887	Fatal Signal 11: smgr_uplane_rule_compare_icmp_type()	cups-up
CSCwe28217	[CUPS UP] sessmgr restart is seen at uplane_free_icmp_session()	cups-up
CSCwf30799	[CUPS UP] UP is not accounting packet in URR after UP switchover for dynamic rule with precedence 0	cups-up
CSCwf23942	ePDG sends invalid S-NSSAI values in IKE_AUTH_RESPONSE even when 5G-IWK feature is not enabled	epdg
CSCwf19626	Backward compatibility of MME (supporting LTE-M) with SGW that does not support LTE-M	mme
CSCwe94309	MME rejecting the service request from NBIoT device in case when eea3 and eia3 is enabled	mme
CSCwf79740	[BP-CUPS]: While performing LTE to WIFI HO observed “CC Req No 1” Error logs continuosly generating	pdn-gw
CSCwe83141	PGW Sends CCR-T when UE is in Assume Positive state and never established a Gy session	pdn-gw
CSCwe59929	Billing Impact caused by Gy CCR-T Request Number incorrectly increases after Assume Positive	pdn-gw
CSCwe45652	PGW is not triggering UBR after RAR from PCRF for IP Filter Replace	pdn-gw
CSCwe64879	Bulkstats are reporting high utilization for DATARATE_IPPOOL schema	pdn-gw
CSCwf17642	The PGW sends a CCR-U with no USU when the Tariff-Time-Change value expires)	pdn-gw
CSCwe21138	BP-ICUPS: sessmgr restart : sfw_nat_allocate_port_chunk_from_recovery_list()	pdn-gw
CSCwe70747	[BP-PGW] Gy_CCR-Termination message AVPs validation is failed post the sessmgr/aaamgr recovery	pdn-gw
CSCwd28893	Shifting to smi-ops-center 2022.03.1 for security fixes	rcm
CSCwc98595	[RCM-PLT]Checkpointmgr stats showing old Active info after the same has become standby	rcm
CSCwd02219	RCM checkpointmgr optimisation for URR handling	rcm
CSCwd61972	Masking Error logs flooding checkpoint manager logs and add counters to display in stats	rcm
CSCwf69438	High CVE in component runc. Upgrade to latest version.	rcm
CSCwd35392	UPF Planned switchover timers need to be configurable (timers on rcm)	rcm
CSCwe39289	"Update stats for planned switchover PreSwoTimeout, FlushChkptTimeout and NonCritFlushChkpt"	rcm
CSCwd20323	Error in tcp client write msg write tcp i/o timeout	rcm
CSCwd79989	checkpoint manager statistics are broken	rcm
CSCwf48020	to integrate fix for Azul Zulu Java Multiple Vulnerabilities (2023-04-18) to RCM ops-center	rcm
CSCwd71343	RCM Bfdmgr - Add diagnostic code to BFD down notification	rcm
CSCwe40715	Missing rcm-controller and rcm-bfdmgr traps in disable-trap list	rcm

Bug ID	Headline	Product Found*
CSCwe78924	Critical CVE in component spring-framework. Upgrade to latest version.	rcm
CSCwe40690	snmp issues in checkpointmgr	rcm
CSCwf40417	Issue while applying host config with “apply_config.sh” script	rcm
CSCwc10201	Race condition in informing RCM HA state from keepalived to controller	rcm
CSCwd94821	chkpointmgr pod restart does not initiate sock conn towards stby sessmgr	rcm
CSCwe40744	Boot Registration and Complete trap for UPF is missing UPF State	rcm
CSCwe42938	Bfdmgr crashloop observed upon changing the timer values	rcm
CSCwd67670	[UPF-RCM]RCM stat 'CurrTotNumCallStats' should be removed.	rcm
CSCwe98183	checkpoint manager stats for invalid callid is needed	rcm
CSCwd63261	Need logs in persistent files in the failing RCM when RCM HA happens	rcm
CSCwe43183	Some UPF specific rcm-controller traps do not show UPF IP address	rcm
CSCwf06065	checkpoint manager level aggregate session stats for different types of checkpoints	rcm
CSCwf59447	rcm-dashboard not up with offline image or with rcm-product	rcm
CSCwf04371	sessmgr restart at acsmgr_clp_send_checkpoint_dcca	sae-gw
CSCwf15441	egtpegmgr restart seen on SPGW after recent SW upgrade.	sae-gw
CSCwe91665	session manager restart at function tfDuplicateSharedBuffer on SAEGW	sae-gw
CSCwf34985	Increased number of Del-bear-requests and Del-Session-Requests seen on S5 and S11 on SAEGW	sae-gw
CSCwh13773	Converged Core Gateway sends RA to the UE but no ipv6 traffic from UE then there is UE disconnect.	upf
CSCwf21120	UPF gtpumgr going to warn/over state with high memory usage	upf
CSCwe33291	[UPF-ST]: Continuous error logs on standby UPF “SMGR ID mismatch during recovery”	upf
CSCwh14297	UPF to have option to ignore OHR IE in Update-Core-PDR in sx-mod-req	upf
CSCwe96265	"[UPF-MONSUB]Exit code in case of converged 4G calls is not correct, monsub enabled using console/smf"	upf
CSCwf14185	[H-SMF] SMF sends Update QER with QFI0 during back to back 4g to 5g roaming handover	upf
CSCwf50873	[UPF-ST-MonSub] : Sessmgr restarted at sessmgr_handle_npu_response_cb()	upf
CSCwh17947	Seen sessmgr restart at sn_memblock_memcache_alloc()	upf

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

Operator Notes

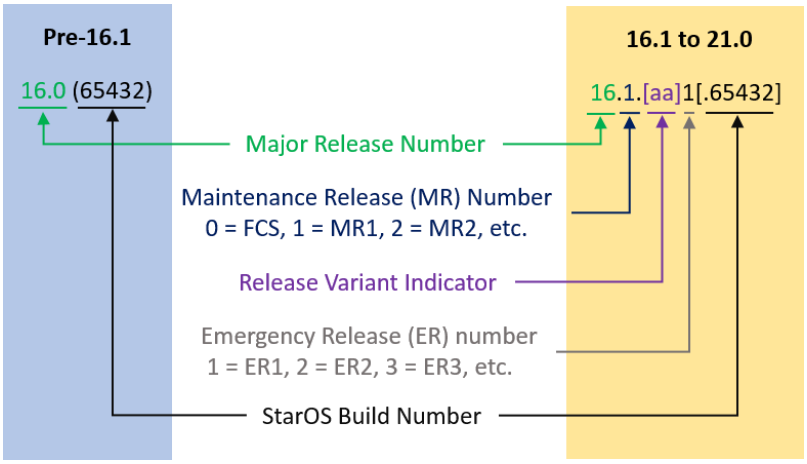
StarOS Version Numbering System

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.

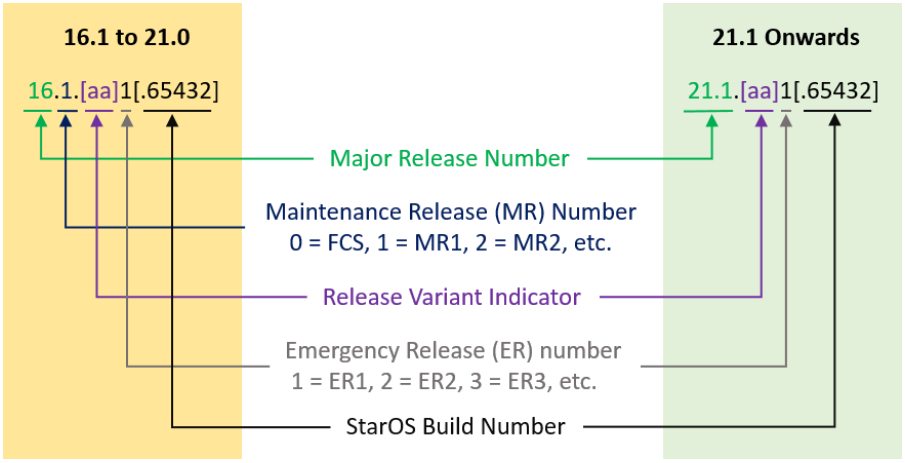
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 5 provides descriptions for the packages that are available with this release.

Table 5 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains 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>.zip	asr5500_T-<release>.bin	Contains 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.
StarOS Companion Package		
companion-<release>.zip	companion-<release>.tgz	Contains 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. In 21.12.0 and later releases, the StarOS companion package also includes 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.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes 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.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains 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. In 21.12.0 and later releases, this package also includes 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-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes 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.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains 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. In 21.12.0 and later releases, this package also includes 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 Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes 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.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 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 6 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 6 - 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 of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone 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. (1721R)