Release Notes for StarOS Software Version 21.23.32

First Published: December 05, 2023
Last Updated: December 05, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.23.31. These release notes are applicable to the ASR5500, VPC-SI, VPC-DI platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.23.32, build 92329

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 http://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.

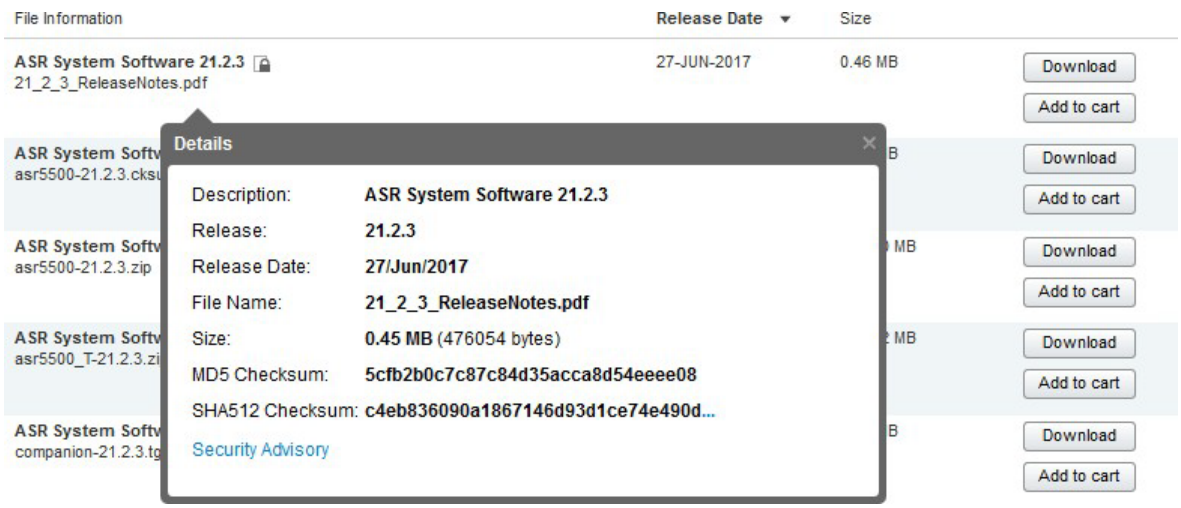
Firmware Updates

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*
CSCwe51501	Call rejections ongoing even when license came back to underlimit after license was breached in CP	cups-cp
CSCwe49912	After second UP (ims) ICSR switchover IMS Media/signaling are not entering the IPSEC tunnel.	cups-cp
CSCwe27712	Behavioural difference between CUPS and NON-CUPS in terms of handling Gy response code 4011	cups-cp
CSCwd76879	Sessmgr process restarted at function sessmgr_compress_call_info()	cups-cp
CSCwd60402	CUPS-CP: Low Throughput - CRBN=Fallback. [project: auto-fallback to local policy]	cups-cp
CSCwc34314	[CUPS UP] Firewall NAT port release behaviour change between legacy and CUPS	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwi32188	[BP-CUPS]: Fatal Signal 11: smp_fp_fill_strm_sfp_mtd() during ICSR switchover with BFD Down	cups-up
CSCwi26307	[BP_CUPS] Downlink packet is not observed on chassis after removing and adding VLANs related to TS	cups-up
CSCwi24925	[BP-CUPS]: vppctl errors seen on UP after Traffic Steering is enabled	cups-up
CSCwf75558	"show subscribers idle-time" displays the incorrect UE sessions	cups-up
CSCwf03068	Rulebase ID change causing rulebase corruption	cups-up
CSCwe85093	UP core files generated after removing ruledefs	cups-up
CSCwe83354	GTPU Test Echoes Received but not Reported to CLI	cups-up
CSCwe28217	[CUPS UP] sessmgr restart is seen at uplane_free_icmp_session()	cups-up
CSCwd40057	After all sessmgr restart, sx-peer-node info is lost on standby chassis	cups-up
CSCwc99110	[BP-CUPS]: Assertion failure at sess/smgr/sessmgr_gtpu.c sessmgr_egtpu_signalling_routine()	cups-up
CSCwc41191	[BP-CUPS][sessmgr 12341 error]<sessmgr:19> essmgr_uplane.c:36963][SXB]Updated URR doesn't exist.0x27	cups-up
CSCwc30206	[BP-CUPS] Smgr restart sn_memblock_cache_get_mcblock_by_addr & sessmgr_uplane_cleanup_gxalias_lists	cups-up

CSCwc17829	[BP-CUPS] Observed smgr crash while connecting a call with gx-alias feature enabled	cups-up
CSCwb78943	[CUPS] Fatal signal 11 - sess_get_next_pdr_info() - smgr_match_pdr	cups-up
CSCwb52197	[CUPS UP] VPP/hatsystem restart clib_memcpy_fast() during IP routes consolidation in BGP,	cups-up
CSCwb07879	LCI/OCI changes CUPS-UP	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCwi10489	sessmgr crashes when customer block/unblock the securenet blades	cups-up
CSCwd16366	LI IPSec tunnel flaps intermittently due to SA Collision	epdg
CSCwc69907	ePDG sessmgr crash on Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:7048	epdg
CSCwe54541	[MME] mmedemux recovery is not supported for ENDC SON feature	mme
CSCwe42649	MME using IPv6 address wrongly during TAU triggered inter-SGW change.	mme
CSCwd97399	Observing mmemgr crash:: cmPAsnDecChExt	mme
CSCwd73793	Assertion failure at sess/mme/mme-app/app/mme_pdn_fsm.c:829	mme
CSCwc83863	Assertion failure at sess/mme/mme-app/app/mme_app_util.c:18558	mme
CSCwc80299	CBC , MME send Write Replace Warning Indication before Write Replace Warning Response	mme
CSCwc59471	sessmgr in warn/over state due to mme_app_allocate_s1nas_msg and SN_cmAlloc()	mme
CSCwc51275	Assertion failure at snutil/sn_memblock.c:310 on vMME	mme
CSCwc43059	sessmgr restart at mme_hss_get_user_data	mme
CSCwc25016	sessmgr restart when provisioned with IPv6 and LI Event Delivery type UDP ACK Format	mme
CSCwb58470	Clear subscriber not working with service still running	mme
CSCwb53675	[MME] release-due-to-pre-emption (39) S1AP radio network cause not implemented	mme
CSCwa93249	MME sessmgr restart seen in Function: mme_app_egtpc_abort_low_priority_trans()	mme
CSCwa92153	Corruption in vpnmgr when large amount of data gets dumped	mme
CSCwa36635	MME crashes after upgrade to v21.23.6_21_mme_fsm_event_handler()	mme
CSCvz90152	SessMgr restart during X2 Handover	mme
CSCwi16827	Sess mgr crash during Delete bearer sess procedure	pdn-gw
CSCwf58752	Truncated dest-host from node on Gx CCR-T's	pdn-gw
CSCwe35187	SessMgr restart seen during the collision scenario for 3g handover	pdn-gw
CSCwd67200	Incomplete MSISDN in servedMSISDN CDR field	pdn-gw
CSCwd44164	sessmgr task unexpected restarted occurred on PGW acs_http_accel_check	pdn-gw

CSCwd32146	"Update Bearer Request" is send PGW->SGW without EPS Bearer QoS, which is not aligned with 3GPP	pdn-gw
CSCwb81718	CCR-U/CCR-T for Non-WPS session going through WPS channel	pdn-gw
CSCwb42809	Nat call object list length going wrong when Insertion failed on NAT call obj list	pdn-gw
CSCwb34009	Fatal Signal 11 in acsmgr_destroy_recorded_adc_flows_list()	pdn-gw
CSCwb23785	Corrupted values of total/output octets displayed in CDR for Ga interface	pdn-gw
CSCwa59860	Sessmgr crashes after p2p plugin update v2.67.1490	pdn-gw
CSCwa52782	Node reloaded after LAG group port reconfiguration	pdn-gw
CSCwa52583	ICUPS : Session Manager restarts on PGW	pdn-gw
CSCwa39302	sessmgr crashes sessmgr_rf_fill_service() Assertion failure at sess/smgr/sessmgr_rf.c	pdn-gw
CSCwa36871	ADC detection degraded for Youtube	pdn-gw
CSCvz02641	Card migration causing BGP failure	pdn-gw
CSCvx61024	sessmgr restart observed at "sn_ext_process_packet"	pdn-gw
CSCwd71343	RCM Bfdmgr - Add diagnostic code to BFD down notification	rcm
CSCwd63261	Need logs in persistent files in the failing RCM when RCM HA happens	rcm
CSCwb12055	CLI to prevent multiple config push notifications towards NSO	rcm
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCvz70919	RCM OVF deployment for 21.25.x image is not succeeding	rcm
CSCvy86141	Add timeout for NSOSim HTTP POST notification [BEMS01305755]	rcm
CSCwe53061	Session manager restart at sessmgr_pgw_create_bearers()	sae-gw
CSCwd64943	[SAEGW] - ASR5500- - 21.23. 12 ICSR Standby sessmgr in Memory over state	sae-gw
CSCwd17939	In sGWRecord, changeTime appearing as before time from recordOpeningTime and duration showing zero	sae-gw
CSCwb58656	sessmgr restart due to Assertion failure at sess/smgr/sessmgr_hlcom.c:467	sae-gw
CSCwb58018	Description of IDFT-support in sgw-service configuration document missing	sae-gw
CSCwb55423	[VPC-DI] Sessmgr process restart at sessmgr_pgw_fill_event_record_csr	sae-gw
CSCwa54898	Sessmgr restart - Fatal Signal 6: PC: [09ed1233/X] acsmgr_adc_dispatch_event()	sae-gw
CSCwa23914	sessmgr restart due Fatal Sig PC: [09fd165b/X] acsmgr_sess_sr_uchkpt_delete_all_accnt_mscc_bucket()	sae-gw
CSCvy78942	With WPS3B configuration GW use secondary PAS during mid-session	sae-gw
CSCwc42261	SGW is rejecting the attach even it is emergency apn/subscriber.	sgw
CSCwd08112	CPVM hanged in context initializing state after CF changeover by DI Internal fluctuation	staros

CSCwa40585	Vpnmgr restart @ vpnmgr_check_addr_conflict()	staros
CSCwa37867	GRE Tunnel with KA not coming up after Card Migration	staros

***** 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*
CSCwh91323	Layer 2 Steering Sending Packets in unexpected direction for Uplink	cups-up
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

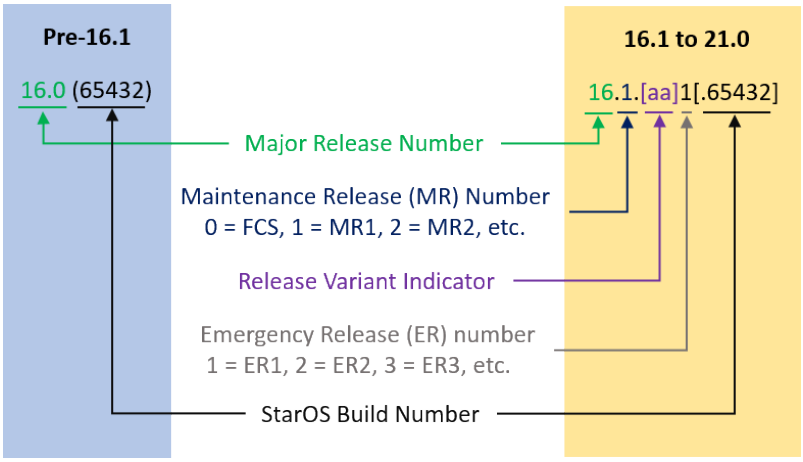
StarOS Version Numbering System

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.

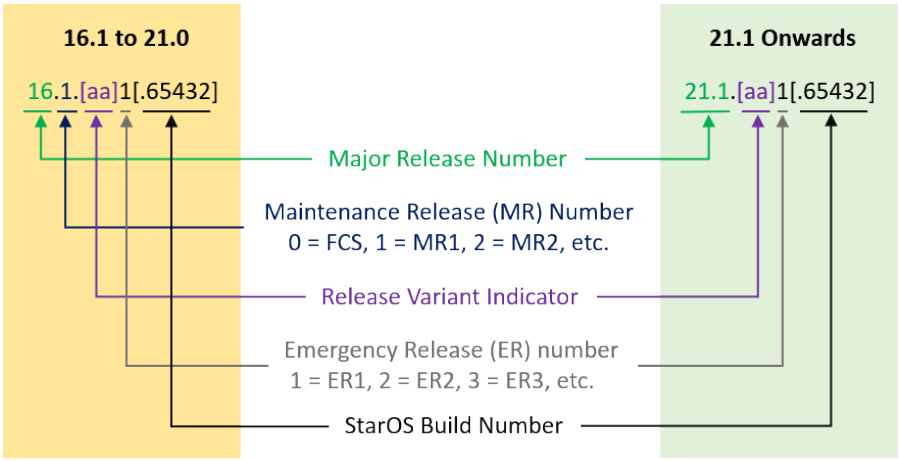
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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