Release Notes for StarOS™ Software Version 21.25.10

First Published: July 13, 2022
Last Updated: July 13, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.25.9. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.25.10, build 86143

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.

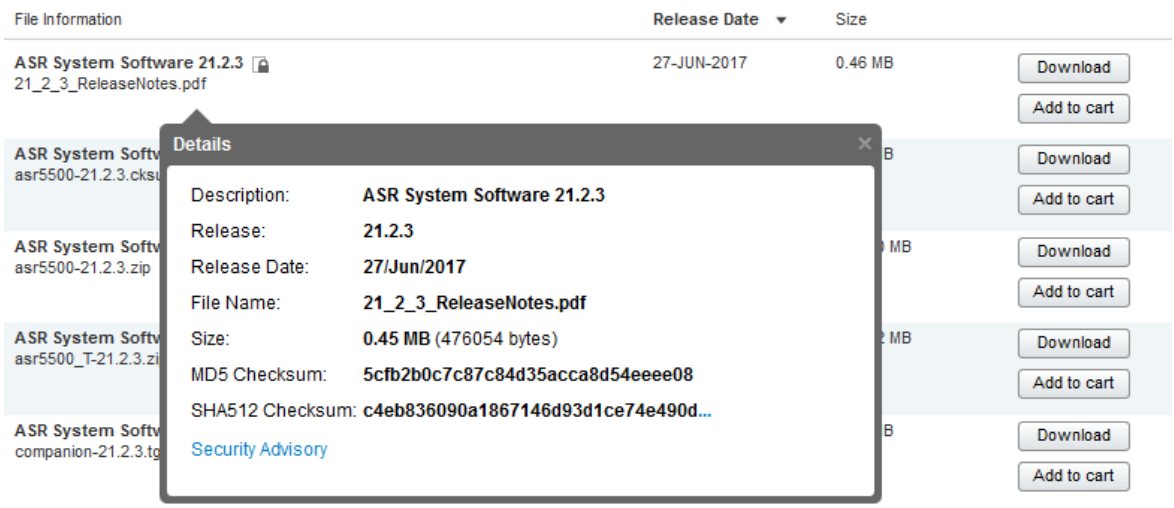
Firmware Updates

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*
CSCwc39963	[Smoke2-Legacy] S8HR Intercepted calls not established after bbiff_trigger	cups-cp
CSCwc18750	ARP Request have wrong Sender IP set to network address instead of interface address	cups-up
CSCwb46218	[BP-CUPS] Crash on sessmgr_uplane_process_sx_sess_modify_request()	cups-up
CSCwb57352	[CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131	cups-cp
CSCwa08379	APN without IP pool name not able to serve call despite having free IPs.	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp
CSCvz92617	[BP-CUPS]:Huge number of error logs observed acsmgr_populate_chrg_info_from_urr failure	cups-cp
CSCwc26989	[BP-CUPS]:Calls are not getting distributed properly on the UPs when there are different versions	cups-cp
CSCwc21399	[BP-CUPS][sx 221332error][<sessmgr:23>sx_db.c:1238]Tunnel_record local seid and Packet seid does not	cups-cp
CSCvz73626	sessmgr assert @ smgr_uplane_config_rule_options()	cups-up
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up
CSCwb55459	[BP-CUPS]:Assertion failure at sctrl_cfg_sync_decode_traffic_optimization_profile_config_tlv()	cups-up
CSCvz49026	[BP-CUPS] sessmgr restart @ sn_memblock_memcache_alloc()	cups-up
CSCwb75761	Multiple session manager restart - sessmgr_process_init_config	cups-up
CSCwc22725	[BP-CUPS][ipsec 56745 error] [sessmgr 11975 error][fapi 223801 error]	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvu18163	Recovery mechanism is not working as expected for CIOT calls after session manager restart	mme
CSCwa46574	PLT-ICUPS-21.26: DNS_KPI_Enhancements - DNS client statistics output is inconsistent	pdn-gw
CSCvz76252	[BP-ICUPS] buffer leak found at VPP with regular callmodel sessions on the chassis	pdn-gw

Bug ID	Headline	Product Found*
CSCvy90872	"BP-ICUPS: VPP restart while running the callmodel, resulted in segmentation fault"	pdn-gw
CSCwa54994	BP-ICUPS: sm reload at sn_memblock_cache_block_flush.part.1()	pdn-gw
CSCwa11844	BP-ICUPS: aaamgrs are going to over state due to high memory usage	pdn-gw
CSCwc25574	[BP-CUPS]Planned UP switchover failing due to "Switchover timer on UPF timed out"	rcm
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCvz61597	[SGIR-Ph1] After first switchover some profiles are in unknown state initially in save & reload case	sae-gw
CSCvz65453	[SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN	sae-gw
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvy50485	[SVI-UPF]: vpp restarts at sn_assert_signal_handler()	upf
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	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*
CSCwc19603	Lower log level for "sessmgr 12241 error"	cups-cp
CSCwc20916	[CUPS CP] Assertion Failure @ sn_slist_lookup_by_key()	cups-cp
CSCwc15578	[CUPS CP] Sx Mod for Li Dup FAR missing when using GGSN Service and Selective LI Encryption	cups-cp
CSCvr98248	"CUPS: sessmgr 10699 error Misc Error: SGW Sx Delete request failed:, error code 1"	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwc12794	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwb41247	[BP-CUPS] Observed smgr restart "smgr_fsm_newstate" on CP on Longevity execution	cups-cp
CSCvy50239	Incorrect number of the active subscriber in show saegw-service statistics	cups-cp
CSCwa14260	"active counter for pure-S is still remained , though call is already purged due to sx-path-failure "	cups-cp
CSCwb56846	[CUPS] data-from/touser-average (APN bulkstat) is still increasing with SGW traffic	cups-cp
CSCwb65661	[CUPS] Fatal signal 6 - sgwdrv_process_egtpc_change_notification_ind	cups-cp
CSCwb87081	[CUPS-CP] Discrepancy between Gy and Gz reporting when "exclude-packet-causing-trigger" configured	cups-cp

Bug ID	Headline	Product Found*
CSCwb89829	[CUPS-CP] Incorrect counting of rejected handovers	cups-cp
CSCwa82550	[CUPS-CP] Discrepancy between Gy and Gz reporting when	cups-cp
CSCwa19731	UP in busyout state get sessions assigned	cups-cp
CSCwa92055	Session is established on busy-out UP under UP re-selection algorithm.	cups-cp
CSCwb63921	sessmgr crash - Assertion failure at sess/smgr/sessmgr_sgw.c:11881	cups-cp
CSCwa32380	Crash seen on CP while executing UE initiated dedicated bearer scenario	cups-cp
CSCwb38173	[BP-CUPS]sessmgr 10396 errors on standby CP.	cups-cp
CSCwb85916	CUPS-CP: Assertion failure at sess/smgr/sessmgr_snx.c:4645	cups-cp
CSCwb33013	Random CRBN/RG mismatch in CDRs	cups-cp
CSCwb75286	Multiple Sessmgr Crash with same crash stack crashed multiple times frequently	cups-cp
CSCwb41424	CUPS CP sessmgr task restart smc_sx_copy_sef_pdu_to_sx_pdu	cups-cp
CSCwb45094	SX_ASSOCIATION_SETUP_REQUEST is rejected by CP after Demux SF unavailability	cups-cp
CSCwb71157	PGW U-addr and SGW U addr for dedicated bearer should be IPv4 if it is created with IPv4 address	cups-cp
CSCwb39582	[CUPS CP] Monitoring key_CP is not reporting the final usage reporting in SX modify response to GX	cups-cp
CSCwb16706	[CUPS] sn_assert() egtpc_handle_rel_access_bearers_rsp_evt() egtpc_handle_user_sap_event()	cups-cp
CSCwb34440	Observing sessmgr crash::sessmgr_sgw_handle_get_peer_profile	cups-cp
CSCwb35130	"CUPS CP : call-waiting service after the PGW <> GGSN handover , kills volte session"	cups-cp
CSCwb32201	CUPS CP imsa_handle_sgx_delete_notify_callback	cups-cp
CSCwb42432	[BP-CUPS]: Fatal Signal 11: 11 PC: [03c4aea6/X] sessmgr_pcc_intf_free_cached_sef_evt()	cups-cp
CSCwb44877	sessmgr Assertion failure at sess/egtp/egtpc/egtpc_interface.c:246	cups-cp
CSCwb02037	CUPS CP : SGW sess current counter show abnormal increase after ICSR switchover	cups-cp
CSCwb23375	"CP sends SX PFD messages, despite 'sx-pfd-push disabled' being configured under the user-plane-group"	cups-cp
CSCwb36835	sessmgr 11176 error: Unhandled Sx Modify Response in Connected state	cups-cp
CSCwa94198	[BP-CUPS]:Sessmgr memory keeps on increasing after add/modify/delete operation	cups-up
CSCwb38623	[BP-CUPS] Observed smgr restart “sessmgr_uplane_process_sx_sess_modify_remove_gx_alias_pdr_list”	cups-up
CSCwc07806	[CUPS-UP] SRP standby SessMgr memory leak	cups-up
CSCwb43121	sessmgr restart at sessmgr_cancel_uplane_dns_query_and_continue	cups-up
CSCwb70785	"CUPS-UP: hatsystem crash due to VPP timeout, Assertion failure at hat/hatsystem_fail.c:2115"	cups-up
CSCwc19840	Unable to browse HTTP sites over CUPS setup with fw-and-nat feature enabled	cups-up
CSCwa49462	[BP-CUPS] Observed Smgr restart “libc.so.6/__memset_sse2_rep” in Longevity setup	cups-up

Bug ID	Headline	Product Found*
CSCwa98318	[BP-CUPS] Assertion failure at Function: sn_memblock_memcache_alloc()	cups-up
CSCwb22363	CUPS UP stuck ICMP NAT port chunks during TOPUP(rulebase change) 21.23.19	cups-up
CSCwb54746	Sessmgr restarted on UP at uplane_check_modify_copy_orig_ip_packet()	cups-up
CSCwa85071	sessmgr restart while parsing uplane http header	cups-up
CSCwb05811	[BP-CUPS]Data browsing impacted due to URR mismatch between cp/up.	cups-up
CSCwb94113	CUPS: Active UP reload due to NPU-VPP keepalive timeout	cups-up
CSCwa99913	Observing sessmgr crash::sessmgr_uplane_cleanup_far_list()	cups-up
CSCwa79275	CUPS CP Sending GoR name in absence of Ruledef in Rulebase and no Ruledef installed for subscriber.	cups-up
CSCwb25436	[CUPS UP] sm restart at uplane_update_packet_stats_chunk()	cups-up
CSCwb79540	Observed crash in eDPG for Emergency call	epdg
CSCwb88450	Assertion failure at ../ipm/ipm/ipm_sad.c:	epdg
CSCwb73691	Handling of ucam_cavecreek_dh_p1_sync()[2995]: cpaCyDhKeyGenPhase1() Failed with Status: -2!	epdg
CSCwb51664	Need associating SMSC Service from specific context support under MME Service.	mme
CSCwc18935	MME not sending RAT type in Modify Bearer Request	mme
CSCvz92101	GRE Small Fragmented Packets Are dropped	pdn-gw
CSCvz54809	Natting not working for some IPv4 addresses	pdn-gw
CSCwa83203	Observing sessmgr restart::sessmgr_egtpu_receive_gtpu_v6_packet	pdn-gw
CSCwa79949	[soltest]: M6 UPF Sessmgr instances stuck in SERVER Mode after SWO	rcm
CSCwa81910	Upgrade packages in RCM	rcm
CSCwb71454	RCM Scripts apply_config.sh and apply_config_v2.sh permissions changed.	rcm
CSCwb61900	SSH is sometimes not accessible after RCM VM boot	rcm
CSCwb73497	RCM VM manual reboot issue	rcm
CSCwb93284	Windows format support for apply_config.sh and apply_config_v2.sh	rcm
CSCwa79949	[soltest]: M6 UPF Sessmgr instances stuck in SERVER Mode after SWO	rcm
CSCwa40146	[LI-PGW] Observed un-expected content buffer stats output	sae-gw
CSCwa12029	MIOs Cards is crashing due to bad minicores	staros
CSCvx35930	Port bitrate default to 10G for virtual ethernet with iftask	staros
CSCwb26977	Enable VPP full core in non-trusted build	staros
CSCwb72252	NYSMFI24 N4 session degradation - SMF sends Sx-rep-Resp with CC-69	upf
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf

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

Operator Notes

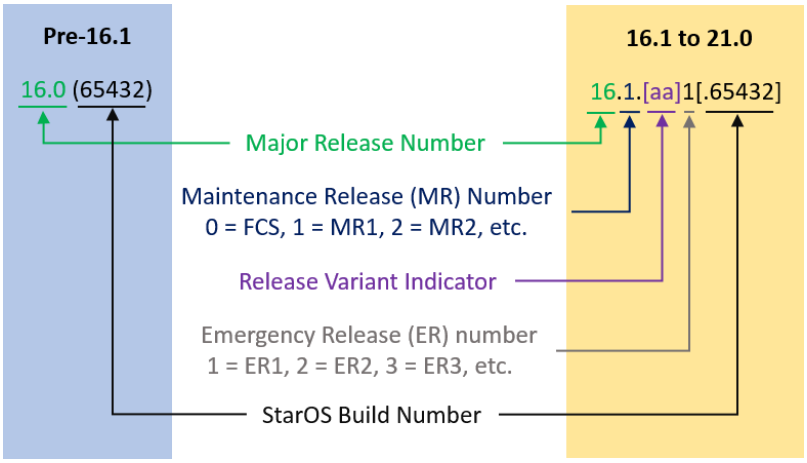
StarOS Version Numbering System

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.

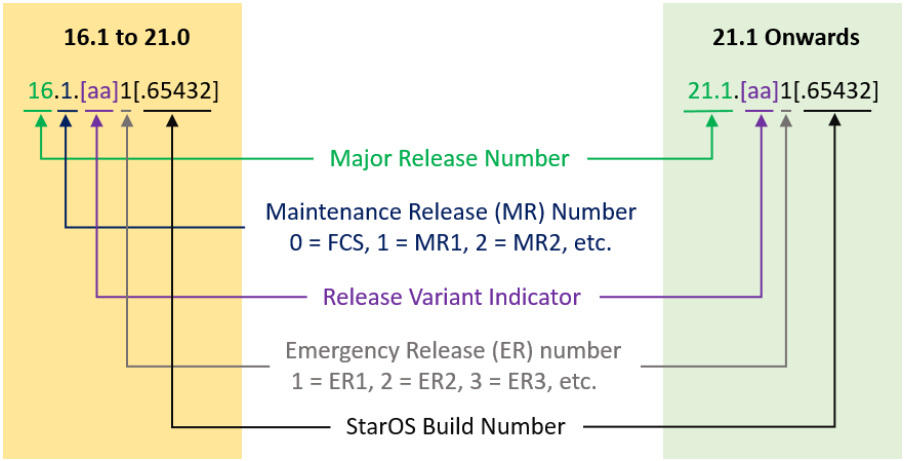
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build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