Release Notes for StarOS™ Software Version 21.22.n13

First Published: February 09, 2023
Last Updated: February 09, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.n12. These release notes are applicable to the ASR5500, VPC-SI , VPC-DI and RCM platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.22.n13, build 88498

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.

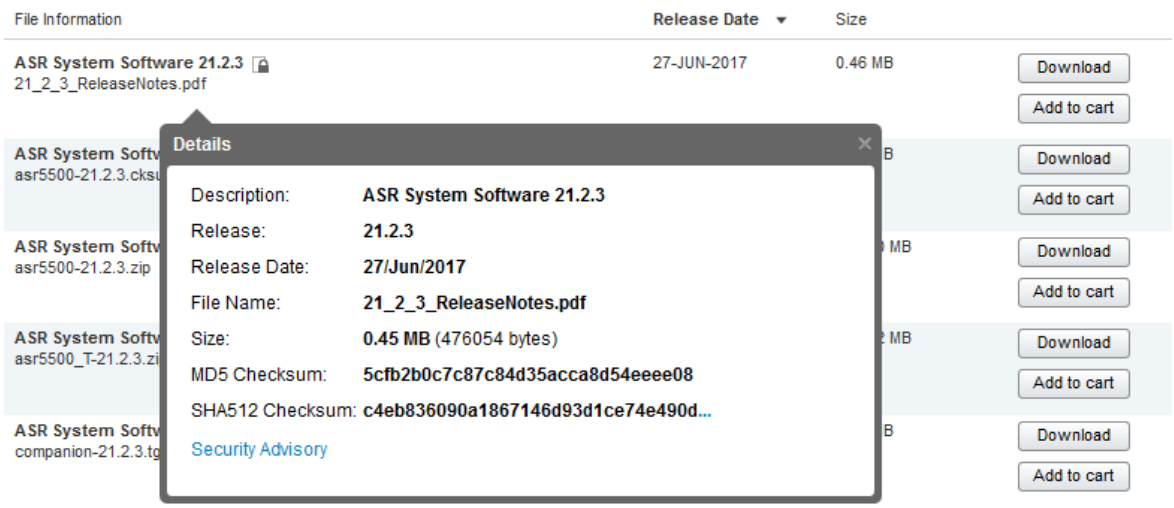
Firmware Updates

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*
CSCwe24070	[BP-CUPS]: sessmgr crash at Function: acsmgr_collect_usage_for_all_monitoring_keys()	cups-cp
CSCvx29537	[BP-CUPS]acsmgr_create_cr_defn()process_install_requests()acs_process_received_policy()	cups-cp
CSCwb57352	[CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131	cups-cp
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running call model	cups-cp
CSCvx75948	[BP-CUPS]:Sessmgr crashes at sessmgr_pgw_handle_ipv4_layer_up()	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp
CSCwd33517	show apn statistics shows wrong value for GERAN and UTRAN users	cups-cp
CSCwd39033	Multiple Sessmgr Crash with function:ipms_flush_hidx	cups-cp
CSCvw83826	[BP-CUPS]: Huge session disconnect with reason “sxfail-opr-remove-pdr”	cups-cp
CSCvt46570	[BP-CUPS]: Huge checkpoint failure at Standby micro-checkpoint failures recovery record not found	cups-cp
CSCvw92011	Subscriber gets disconnected when gx-alias GoR's with shared ruledefs are removed & added via RAR	cups-cp
CSCvx33850	Rulename associated with PDR is not displayed in “show cli” output	cups-cp
CSCvz01552	[BP-CUPS]:IP Pool is in disabled state	cups-cp
CSCwa29010	[BP-CUPS] “show config error” does not show errors.	cups-cp
CSCvy06009	[BP-CUPS] crash acsmgr_vogx_fill_and_associate_urrs_for_existing_pdrs observed in Longevity run	cups-cp
CSCwc19599	Gy credit control failure handling not working when Gy link is down between CP and OCS	cups-cp
CSCwd27672	[BP-CUPS]:Assertion failure at Function: sn_memblock_memcache_alloc()	cups-cp
CSCwd96839	CP triggers CCRU with RESOURCE_ALLOCATION_FAILURE performing 4gto3g Qos Change	cups-cp
CSCvx35192	[BP-CUPS]:Sessmgr Crashes at acsmgr_activate_predef_rule_or_group()	cups-cp
CSCwe30323	[BP-CUPS]: Error logs Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=6	cups-cp

Bug ID	Headline	Product Found*
CSCvy89140	Calls fail with Invalid-dest-context due to VRF id mismatch	cups-cp
CSCvy80968	[BP-CUPS]:[N-1][N-2]Downgraded new standBy UP leads to all call loss once performed UP switchover	cups-up
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCwc02727	[SVI] VPP Crash observed vlib_register_node() unix_cli_file_add.isra.6.constprop.21()	cups-up
CSCwa30749	[BP-CUPS]Continuous error logs- 'In smgr_uplane_compare_tcond_cf_policy_id returning false]'	cups-up
CSCvy57500	[BP-PCT] Incorrect bytes and pkts seen for http analyzer stats.	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCvy51207	[CUPS] Firewall dropping traffic on UP	cups-up
CSCwa18164	Counter rolls over frequently due to inappropriate data-type (e.g. sgw-datastat-dl-qci8totbyte)	cups-up
CSCwd88991	[CUPS-UP]: Packets stats not coming correct after quota exhaustion for TCP v4 traffic	cups-up
CSCvw16587	[CUPS-UP] pure-S_UP crash in smgr_uplane_update_opt_list	cups-up
CSCvy19871	[BP-CUPS]:Assertion failure at sn_memblock_memcache_alloc() on UP	cups-up
CSCwd51494	IPsecMgr task restart while decrypting packets.	epdg
CSCwa75811	For 3G to 4g TAU for DECOR subscriber MME is introducing 10s delay for SGSN context request message	mme
CSCvx53094	sessmgr restart seen in function mme_app_fill_s1_bearer_values()	mme
CSCvz67021	Associating GTPU service to S11 egtp-service casue outage_need to document in MME	mme
CSCvy02339	Parameters are encoded wrongly at MME and sent to GMPC server	mme
CSCvy81235	[DOCBUG] “MME Bearer Request Message During Handover Process” feature activation impact	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvy61494	multi fault with sessmgr restart Function: mme_app_fill_s1_bearer_values()	mme
CSCvy96788	[CUPS-CP] CLI stuck on `show active-charging sessions full imsi <imsi>	pdn-gw
CSCwe21674	Authentication Failing during UDP Socket Creation when using IP VRF Forwarding	pdn-gw
CSCwc31700	“ecs-rbase-sess-cur” in ECS schema has abnormal value	pdn-gw
CSCvx41412	Green peer sometimes not selected when a single host is configured in a row	pdn-gw
CSCwd02729	Continuous EGTPCPathFailClear traps after receiving echo requests during no session	pdn-gw
CSCvw25217	BP-ICUPS : sessctrl crashes during boot up at acs_sanitize_a_single_tdb	pdn-gw
CSCvx37363	[BS-ICUPS] I-951 “PGW-Buffer Merge Count” incrementing wrongly in some error scenarios	pdn-gw
CSCwe25042	[PLT-RCM] rcm show-statistics bfdmgr not working in 21.22.x	rcm
CSCwb73497	RCM VM manual reboot issue	rcm
CSCvx56170	RCM logs show UP password in clear text	rcm

Bug ID	Headline	Product Found*
CSCvx18307	rcm show-statistics controller => last_event_ts NOT updated on UPF reload	rcm
CSCvx07498	[PLT-CUPS]: configmgr and bfdmgr printing garbage logs with K8s	rcm
CSCvx34687	Fix up permissions on /etc/kubernetes/admin.conf	rcm
CSCvz20064	[CUPS RCM] Missing UPs in configmgr after RCM HA switchover	rcm
CSCwc35815	AcsMgr error DNS snooping: unexpectedly p_hentry is NULL	sae-gw
CSCvw58020	Non WPS session : PGW not responding to MBReq - SRVCC without PS handover	sae-gw
CSCvy33792	[VPC-DI] SAMOG Increase cisco-mpc-protocol-interface AVP length for eogre_pmipv6	samog
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvy02352	Parameters are encoded wrongly at SGSN and sent to GMPC server	sgsn
CSCwc69565	[S8HR] show lawful-intercept s8hr statistics all display the wrong ebi value	sgw
CSCvz64429	Failed to load MIB modules from starent.my error	staros
CSCvx70054	bulkstat memory usage increased more than 100%	staros
CSCwa12029	MIOs Cards is crashing due to bad minicores	staros
CSCvx98394	snmpv3 alarms broken after upgrade to 21.22.3	staros
CSCvz46069	IPv6 Mgmt IP not reachable after CF switchover	staros
CSCvy77792	vpnmgr restart seen @ sn_slist_lookup_by_key()	staros
CSCwd75750	ipsecmgr_process_crashed at ipm_sad	staros
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf
CSCvy34368	[GR-SVI] SM restart on UPF at sessmgr_handle_gtpumgr_wrong_sess_replacement	upf
CSCvz80896	Next-hop row is not created if next-hop cli is added in middle of the call	upf
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	upf
CSCwa75370	[Combo-UPF] Uplink data is not getting offloaded after Converged to Non-Converged SGW Relocation	upf
CSCwb21297	Sx TX HB Request count not increasing on CNDP DATA UPFs	upf
CSCvy27480	[UPPF-SVI]:sessmgr restarts at sx_tun_fsm_handle_sess_mod_rsp_evt() during 60 hours on call mode run	upf
CSCvz24037	[UPF-SVI] sessmgr crashed at sessmgr_uplane_interconnect_call_for_combo().	upf
CSCvy34465	[GR-SVI] SM restarts on UPF at uplane_drv_handle_events_from_egtpu_app	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*
CSCwd20301	[BP-CUPS] SessMgr restart due to corruption when processing secondary RAT records	cups-cp
CSCwa86579	Observing sessmgr crash on CP | ggsnapp_process_snx_abort_sub_sess()	cups-cp
CSCwd75222	[BP-CUPS] Observed smgr restart "acsmgr_allocate_cups_sef_info" in ML execution	cups-cp
CSCwd56601	[CUPS] Assertion failure Function: sn_memblock_cache_get_mcblock_by_addr_slow()	cups-cp
CSCvx73208	[BP-CUPS] SessMgr restart at acs_cups_fill_bucket_id_type() while recovering null variable	cups-cp
CSCwd80515	PGW not binding Gx Dynamic rule for dedicated bearer in WiFi to LTE handoff scenario	pdn-gw
CSCwd43478	PGW rejecting create_Session_Req even if SGW is sending a Conditional/Optional IE	pdn-gw
CSCwb58656	sessmgr restart due to Assertion failure at sess/smgr/sessmgr_hlcom.c:467	sae-gw
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

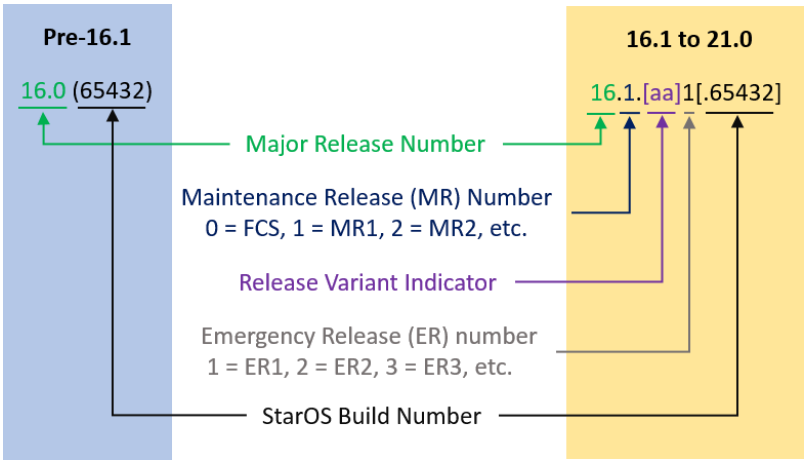
StarOS Version Numbering System

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.

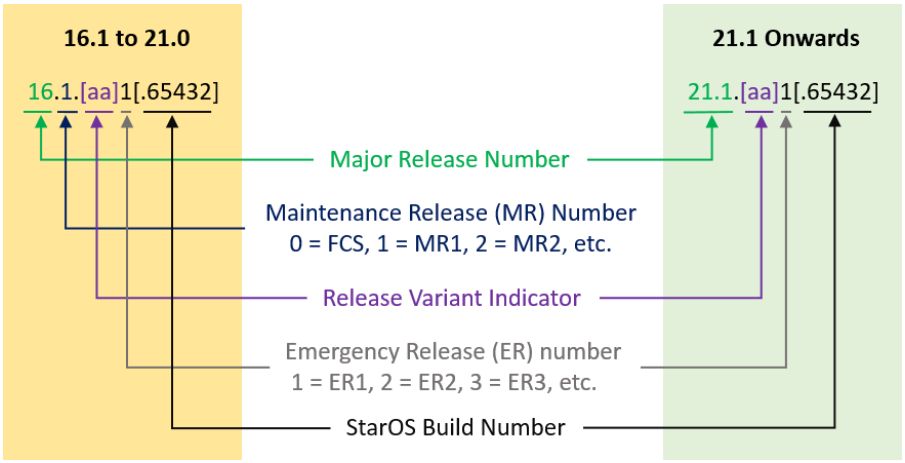
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.