Release Notes for StarOS™ Software Version 21.22.12

First Published: February 04, 2022
Last Updated: February 04, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.8. 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	21.22.12, build 83839

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.
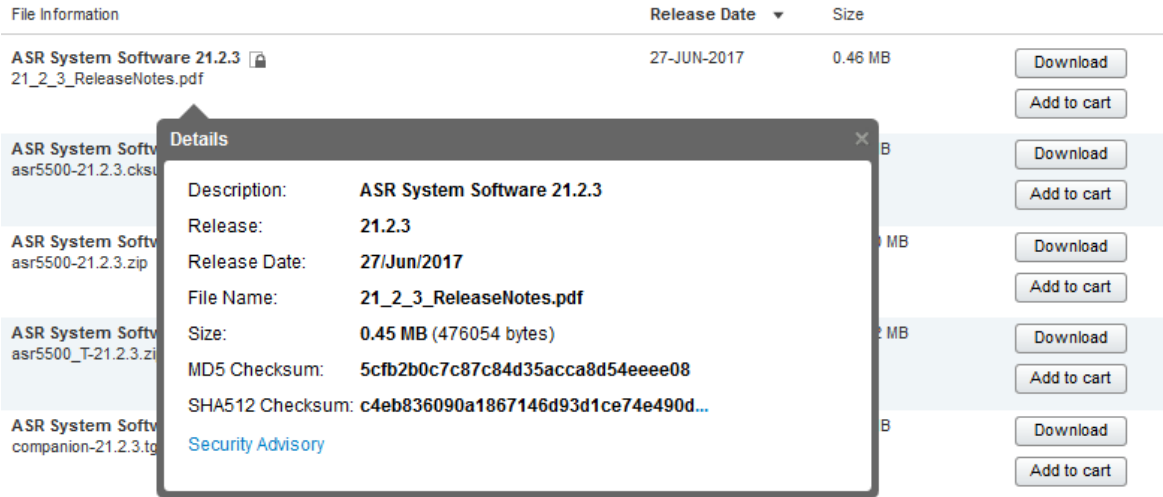
Firmware Updates

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.

File Information	Release Date ▼	Size		
ASR System Software 21.2.3 🔒 21_2_3_ReleaseNotes.pdf	27-JUN-2017	0.46 MB	Download	Add to cart

Details ✕

Description:	ASR System Software 21.2.3
Release:	21.2.3
Release Date:	27/Jun/2017
File Name:	21_2_3_ReleaseNotes.pdf
Size:	0.45 MB (476054 bytes)
MD5 Checksum:	5cfb2b0c7c87c84d35acca8d54eeee08
SHA512 Checksum:	c4eb836090a1867146d93d1ce74e490d...

Security Advisory

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*
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running BYT call model	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp
CSCvx33850	Rulename associated with PDR is not displayed in "show cli" output	cups-cp
CSCvw83826	[BP-CUPS]: Huge session disconnect with reason "sxfail-opr-remove-pdr"	cups-cp
CSCvx28193	"Sessmgr restart in sn_memblock_memcache_alloc, sxmgr_allocate_pfcp_peer_trans_entry on UP ICSR"	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
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCvx53094	sessmgr restart seen in function mme_app_fill_s1_bearer_values()	mme
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvy02339	Parameters are encoded wrongly at MME and sent to GMPC server	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
CSCvw25217	BP-ICUPS : sessctrl crashes during boot up at acs_sanitize_a_single_tdb	pdn-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
CSCvz64429	Failed to load MIB modules from starent.my error	staros

Bug ID	Headline	Product Found*
CSCvy77792	vpnmgr restart seen @ sn_slist_lookup_by_key()	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*
CSCvy87801	[CUPS]memory leak on functions acsmgr_allocate_cups_info() and acsmgr_allocate_cups_sef_info()	cups-cp
CSCvy95539	[CUPS-CP] "show lawful-intercept full all" output is not displaying CC related information	cups-cp
CSCvz87978	[BP-CUPS] UP SGW data statistic counters showing double the value	cups-cp
CSCvy95443	Memory leak observed upon session reconnection radius off / on" resiliency tes	cups-cp
CSCvz60262	[BP-CUPS] Task restart during handover on sessmgr_saegw_update_upper_call_handle_in_driver	cups-cp
CSCvy78249	CCR-U does not have RSU when responding to a RAR	cups-cp
CSCvz26308	CUPS SGW Crash smc_sxa_fill_sess_modify_req_trgr_cbrsp()	cups-cp
CSCvz00059	CUPS CP SM restart at API sgwdrv_process_egtpc_delete_bearer_ind()	cups-cp
CSCvz12277	CP sessmgr restart seen in acsmgr_dcca_process_msccs()	cups-cp
CSCwa55153	[CUPS CP] "discard-traffic" option inside CCFH Template not working as expected for IPv6	cups-cp
CSCvy78310	FUI-Terminate 4012 issues on CUPS	cups-cp
CSCvz38631	[CUPS CP] micro checkpoint failures and sessmgr 10396 error on standby CP	cups-cp
CSCvz53559	[CUPS] [SXB] Remove and Update PDR both present with FAR ID xxx	cups-cp
CSCvz49537	[CUPS-CP] sessmgr restart is seen at Function: sgwdrv_allow_sm_event_in_assert_hit()	cups-cp
CSCvz60643	sessmgr restart sgwdrv_send_create_session_rsp_failure	cups-cp
CSCwa18888	[CUPS CP] Missing Action priorities on UP side after Push Config from CP to UP	cups-cp
CSCvy19306	High Memory usage on CP due to NAPTR Failures	cups-cp
CSCvz29309	Multiple sessmgr restart is seen with sessmgr_pgw_find_trans_info_node_by_proc_type()	cups-cp
CSCvz78239	CUPS CP SM restart at acsmgr_allocate_cups_sef_info()	cups-cp
CSCwa00451	[BP-CUPS] Speed remains at 472 kbps after 2G->4G HO	cups-cp
CSCwa07182	[CUPS CP]After session recovery CP is not shairing Validy Time (time quota) to UP	cups-cp
CSCwa17341	[BP-CUPS]:Sxdemux crashed at function sn_memblock_memcache_alloc() which resulted in session loss	cups-cp
CSCvy98006	Incorrect timestamp in CDR after unplanned SF migration	cups-cp

Bug ID	Headline	Product Found*
CSCvz07258	Gy servers-unreachable not working for CUPS - Session terminated for CCR-I	cups-cp
CSCvz67952	sessmgr restart during PDN releasing connection procedure	cups-cp
CSCvz07294	Gy servers-unreachable not working for CUPS - Use of after-timer-expiry does not create any SU_URR	cups-cp
CSCvz58375	[CUPS CP] "discard-traffic" CLI not supported inside Failure Handling Template	cups-cp
CSCwa47719	Fatal Signal 11: 11 PC: [0927f5e2/X] acsmgr_dcca_message_cb()	cups-cp
CSCvs30808	[BP-CUPS] calls disconnected with reason graceful-cleanup-on-audit-fail after srp switchover	cups-up
CSCvw75999	[BP-CUPS] CUPS config push failed with specific configuration	cups-up
CSCvz98048	[CUPS UP] - Bulk statistics file contains only 50 rulebases for rulebase schema	cups-up
CSCvy50850	[BP-CUPS] sessmgr restart "snx_uplane_driver_event_control_dispatch" during Longevity run	cups-up
CSCvz26137	[CUPS UP] - MSID Information disappears from "show sub all" after SRP Switchover	cups-up
CSCvz44817	CUPS UP - sessmgr crash in uplane_p2p_update_stats	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCwa59048	Multiple crashes in UP nodes	cups-up
CSCvz11048	user-plane-service statistics shows wrong counter value for Sxab interface-type PDNs	cups-up
CSCvz61356	[BP-CUPS] Session manager memory spike during ECS configuration change	cups-up
CSCvy45030	Sessmgr memory increasing on ASR5500 due to smc_sx_allocate_subsession_sx_data()	cups-up
CSCvz21270	[BP-CUPS]UP was still in association state after CP reload	cups-up
CSCvw86791	call failure - v6 static allocation failure seen on UPF	cups-up
CSCvz83292	Mismatch in PDNs total count vs (IPv4+IPv6+IPv4v6 PDNs) & Sxab interface-type PDNs count (CUPS-UP)	cups-up
CSCvw60309	CUPS SRP over IPSEC - UPIMS - Periodic SRP flaps - need for cli to set mtu at context level	cups-up
CSCvz97499	Sessmgr stuck in SERVER mode	cups-up
CSCvy78420	sessmgr restarts at uplane_update_packet_stats_chunk	cups-up
CSCwa68973	Memory Leak Leading to Sessmgr Restarts in CUPS	cups-up
CSCvy83173	CUPS UPF rulebase statistics limited to 50 rulebases	cups-up
CSCvz64067	[BP-CUPS] Observed sessmgr restart "sx_tun_fsm_handle_sess_del_req_msg" in Longevity run	cups-up
CSCvz69172	PLT-ICUPS : Name of bulkstats variables changes after mru_exceeded counter changes	pdn-gw
CSCwa53385	[BP-ICUPS]: srp config checksum error due to extra space after "traffic-optimization-policy default"	pdn-gw

Resolved Bugs in this Release

| Bug ID	Headline	Product Found*
CSCvx66315	Duplicate charging id seen during ICSR upgrade scenario	pdn-gw
CSCvz88656	BGP prefix-count is decremented while its value is already zero	pdn-gw
CSCvz89198	Charging-rule-removal RAR for NPLI doesnt trigger Update Bearer with Ret-Loc	pdn-gw
CSCwa12377	sessctrl restart on standby after reboot	pdn-gw
CSCvz38569	BP-ICUPS : Incorrect reporting of Time-First-Usage AVP in the RF records	pdn-gw
CSCvz82295	BP-ICUPS: sm crashes at acsmgr_fp_get_gy_quota	pdn-gw
CSCwa20640	QvPC-DI : sessmgrs restart while clearing the sessions from the chassis	pdn-gw
CSCvy98310	BP-ICUPS: sessmgr restart while running callmodel with SRP switchovers at 30 mins interval	pdn-gw
CSCvz82132	RCM : Helm privilege improvements	rcm
CSCvz90288	Running apply_config.sh from different directories	rcm
CSCvz22700	SSD cli process reloads with show diameter route table debug-info	sae-gw
CSCvz34526	[SGW-S8HR] Extra bytes seen in IMS Signaling/Media Messages	sgw
CSCvz34975	[S8HR LI] Message TLVs Endianness and Format corrections	sgw
CSCvz58034	[S8HR-Legacy] BBIFF Intercepted details are cleared on sessmgr recovery	sgw
CSCwa26110	[S8HR] enable S8HR only for roaming	sgw
CSCvw74776	VPNMGR process restart during Session Redundancy Test in SVI Testbed	staros
CSCwa17461	Fix for incorrect 21.22.n5 MIB file	staros
CSCvy99060	[CUPS UP] - UP not able to reach NTP Server	staros
CSCvz96864	CAF2 reports false CAF_CRC_FAILURE/CAFPRGERR	staros
CSCvz60492	OpenStack OSP16 - Add support in StarOS ‘tty-inactive’ script to handle this missing serial console	staros
CSCvx98495	[UPF-SVI] : sessmgr restarted at uplane_p2p_update_stats()	upf
CSCvy79875	[UPF-SVI]:multiple session mgr restarts at uplane_icmp_pkt_inspection()	upf
CSCwa60130	[UPF]Uplink stream in preactive state leading to packets stuck in vpp.	upf
CSCwa17946	UPF : File descriptor leak in local context vpnmgr:1.	upf
CSCvx12704	[SVI-UPF]sessmgr restart at PC: [06344731/X] freebuf()	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".
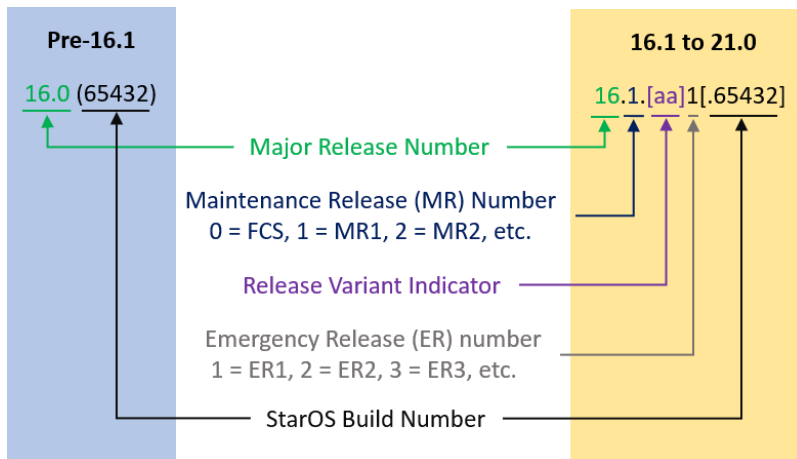
The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".
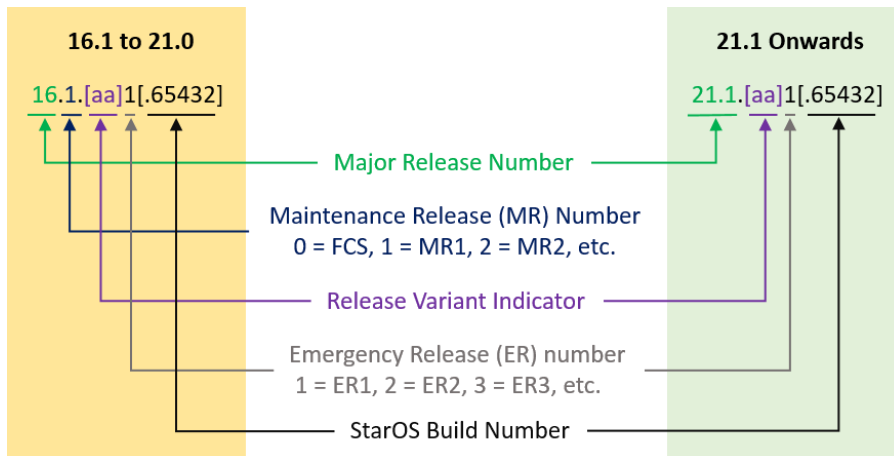
In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

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.