Release Notes for StarOS™ Software Version 21.22.n5

First Published: October 14, 2021
Last Updated: October 14, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.n4. 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.n5, build 82612

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.

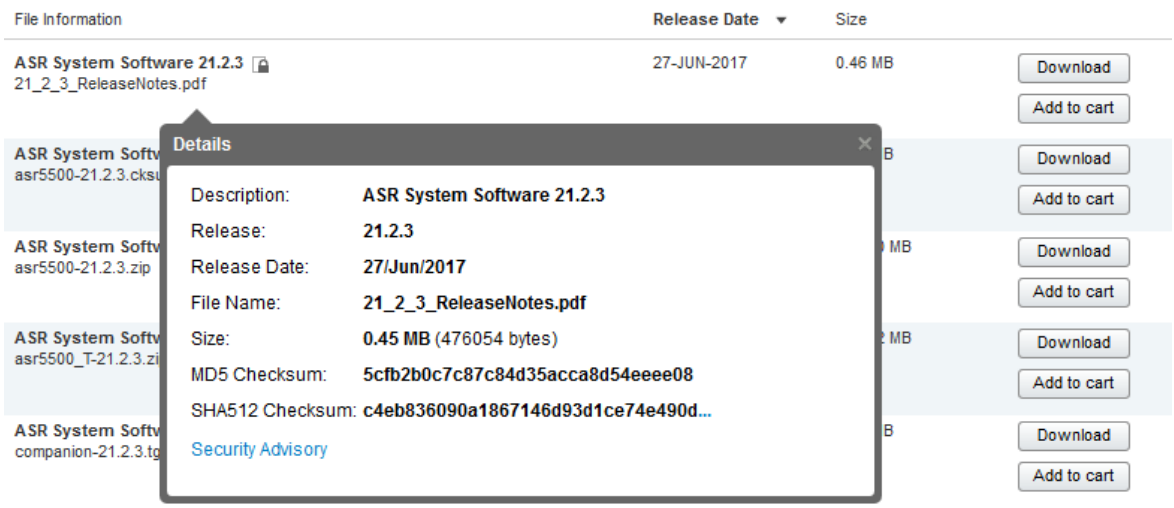
Firmware Updates

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*
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
CSCvz29030	Multiple error logs observed	cups-cp
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCvx28193	"Sessmgr restart in sn_memblock_memcache_alloc, sxmgr_allocate_pfcp_peer_trans_entry on UP ICSR"	cups-up
CSCvz82528	Delay to establish X3 connection after UP DATA switchover	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvy02339	Parameters are encoded wrongly at MME and sent to GMPC server	mme
CSCvx53094	sessmgr restart seen in function mme_app_fill_s1_bearer_values()	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
CSCvs65289	[BP-ICUPS]:Policer row not created in one direction for accelerated flow	pdn-gw
CSCvs65524	[BP-ICUPS] HSUE UDP data not getting offloaded to VPP post RAR with MBR change	pdn-gw
CSCvy13275	show lawful-intercept imei returns No matching LI session/trigger found with active data session	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

Bug ID	Headline	Product Found*
CSCvy02352	Parameters are encoded wrongly at SGSN and sent to GMPC server	sgsn
CSCvz34975	[S8HR LI] Message TLVs Endianness and Format corrections	sgw
CSCvz67912	[S8HR-Legacy] Observed sessmgr crash on ICSR switchover and cli crash on executing S8HR show command	sgw
CSCvy77792	vpnmgr restart seen @ sn_slist_lookup_by_key()	staros
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	upf
CSCvy83156	UPF not detecting the path failure for one of the SMF peer in Multi SMF peer connectivity	upf
CSCvy84329	[SVI-UPF] egtpu_process_invalid_evt()	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*
CSCvy66117	CUPS Gy Failure-Handling for cause-4999	cups-cp
CSCvy87801	[CUPS]memory leak on functions acsmgr_allocate_cups_info() and acsmgr_allocate_cups_sef_info()	cups-cp
CSCvy97261	vpnmgr_cups_add_assign_addresses() restart is seen on CP	cups-cp
CSCvx54858	[CUPS CP] GGSN sends CPC Response with Tunnel ID Data I: 0x00000000	cups-cp
CSCvx93279	SAEGW:DI:CP ->cups, Not able to scale the ceps rate when we have enabled Sx over IPSec.	cups-cp
CSCvy78310	FUI-Terminate 4012 issues on CUPS	cups-cp
CSCvz53559	[CUPS] [SXB] Remove and Update PDR both present with FAR ID xxx	cups-cp
CSCvv94329	[CUPS CP] [N+2 UP Redundancy] - (MonPro) Impossible to delete a Monitor Group	cups-cp
CSCvy02620	[CUPS] [PGWCDR] - causeForRecClosing set to “Normal Release” when Sx Path Failure occurs in 3G/2G	cups-cp
CSCvy14092	[BP-CUPS] vpnmgr crash at vpnmgr_get_loc_vpn_chunk_details_by_vpnid	cups-cp
CSCvy36038	CUPS CP Adds Null Value 0.0.0.0 as the servingNodeAddress in PGW-CDR	cups-cp
CSCvy71912	[CUPS] Monitoring-key not pushed to standby UPF	cups-cp
CSCvy00866	Zero quota preemptively-request scenario CP is sending SX modify for PDR which was never created #2	cups-cp

Bug ID	Headline	Product Found*
CSCvw55567	[CUPS] APN AMBR modification is not applied to existing PDN session	cups-cp
CSCvx78549	[BP-CUPS] Observed restart sessmgr_pgw_fill_pgw_trans_node_from_sx_sef_out_info in Longevity run	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
CSCvz07294	Gy servers-unreachable not working for CUPS - Use of after-timer-expiry does not create any SU_URR	cups-cp
CSCvx45677	[CUPS] [SGWCDR] - Missing “RANSecondaryRATUsageReport” inside SGWCDR	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
CSCvx01746	[CUPS] sessmgr restart Fatal Signal 11: 11 : acsmgr_allocate_cups_sef_info()	cups-cp
CSCvz29309	Multiple sessmgr restart is seen with sessmgr_pgw_find_trans_info_node_by_proc_type()	cups-cp
CSCvx11934	[CUPS ECS] - “flow limit-for-flow-type” and “flow limit-for-bandwidth id” are used together	cups-cp
CSCvz07258	Gy servers-unreachable not working for CUPS - Session terminated for CCR-I	cups-cp
CSCvy17556	"CUPS-CP: with address-hold-timer in pool config, “current sessions” count in 'show sx peer' is wrong"	cups-cp
CSCvy63788	Loss of LI X1 connection after CP reboot	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
CSCvo47185	[BP-CUPS]Tos marked downlink pkts are counted twice in show sub cli.	cups-up
CSCvw75999	[BP-CUPS] CUPS config push failed with specific configuration	cups-up
CSCvw43171	[CUPS] [PFD Management] - Inconsistent rulebase configuration between CP & UP	cups-up
CSCvx35184	CUPS-UP & UPF:UPF not sending Sx_report on time threshold.	cups-up
CSCvy21423	[CUPS] Task restart while config is applied to UP #03	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
CSCvw04208	show subscribers user-plane-only callid <id> qos-group statistics not giving correct o/p on v21.x.gx	cups-up
CSCvw71600	[CUPS] vpp_output.log size growing to 1GB - causes no space left on device - sessmgr crash observed	cups-up
CSCvy50850	[BP-CUPS] sessmgr restart “snx_uplane_driver_event_control_dispatch” during Longevity run	cups-up

Bug ID	Headline	Product Found*
CSCvw76282	[CUPS-UPF] Multiple sessmgr crashes on UP	cups-up
CSCvw97371	[BP-CUPS] SessMgr restart dut to Fatal Signal while changing action priority for a rule	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCvw91153	[CUPS-UP] Source IP violation packet is counted twice in CUPS for an IPv6 session	cups-up
CSCvy39181	inner-fragmentation support is required if DF bit is set in the received packet	cups-up
CSCvy83173	CUPS UPF rulebase statistics limited to 50 rulebases	cups-up
CSCvx32800	[CUPS / UPF-DATA] Fatal Signal 11 at sessmgr_uplane_readdr_adf_compare_hash_entry	cups-up
CSCvz64067	[BP-CUPS] Observed sessmgr restart “sx_tun_fsm_handle_sess_del_req_msg” in Longevity run	cups-up
CSCvs23558	[BP-CUPS] PC: [048dd1d7/X] smgr_uplane_handle_config_chrg_action()	cups-up
CSCvy57179	Incorrect MEMIF - BIA mapping in the FIB Table	cups-up
CSCvy62199	[sol test] SM restart with fun: uplane_populate_edr_field_http_header_len()	cups-up
CSCvw60309	CUPS SRP over IPSEC - UPIMS - Periodic SRP flaps - need for cli to set mtu at context level	cups-up
CSCvx97927	[CUPS UP] - UP stuck in “UAANEPU” state after CP Reload	cups-up
CSCvy78420	sessmgr restarts at uplane_update_packet_stats_chunk	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
CSCvz69172	PLT-ICUPS : Name of bulkstats variables changes after mru_exceeded counter changes	pdn-gw
CSCvx66200	[BP-ICUPS]:SM crashes observed on active and standby with “acsmgr_deallocate_call_obj()”	pdn-gw
CSCvy30776	Wrong CDRs are generated by PGW on receiving Secondary RAT Usage Reports in CNR	pdn-gw
CSCvz00817	BP-ICUPS: Continuous VPP restart resulted in segmentation fault and callmodel failing	pdn-gw
CSCvz82132	RCM : Helm privilege improvements	rcm
CSCvz34526	[SGW-S8HR] Extra bytes seen in IMS Signaling/Media Messages	sgw
CSCvz58034	[S8HR-Legacy] BBIFF Intercepted details are cleared on sessmgr recovery	sgw
CSCvy12988	Wrong CDRs are generated by SGW on receiving Secondary RAT Usage Reports	sgw
CSCvu89348	%rxdiscpackets% and %txdiscpackets% from incremented with RX & TX OverSize frames	staros
CSCvx98820	[CUPS-TACACS-IPsec] TCP connection failure with second tacacs server during failover	staros
CSCvw74776	VPNMGR process restart during Session Redundancy Test in SVI Testbed	staros
CSCvx60252	[CUPS-CP]: iftask crash on CUPS CP resulting in ICSR switchover	staros
CSCvy99060	[CUPS UP] - UP not able to reach NTP Server	staros

Bug ID	Headline	Product Found*
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
CSCvx60658	[SVI-UPF]:Continuous sessmgr restart at sess/egtp/egtpu/egtpu_session.c:808	upf
CSCvy79875	[UPF-SVI]:multiple session mgr restarts at uplane_icmp_pkt_inspection()	upf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

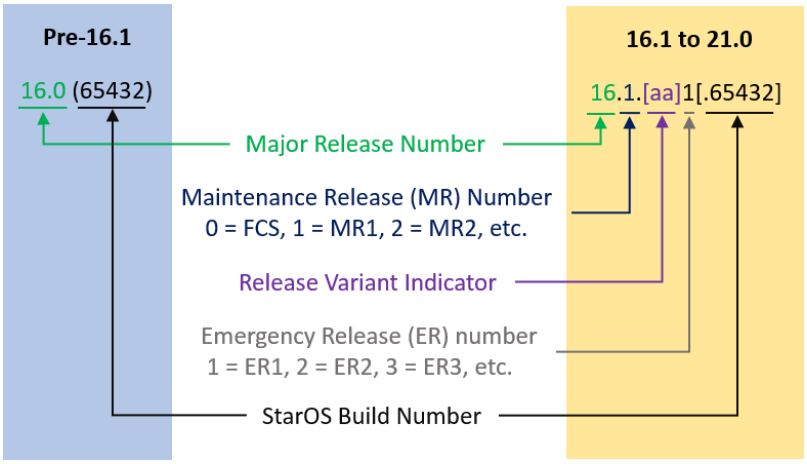
StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

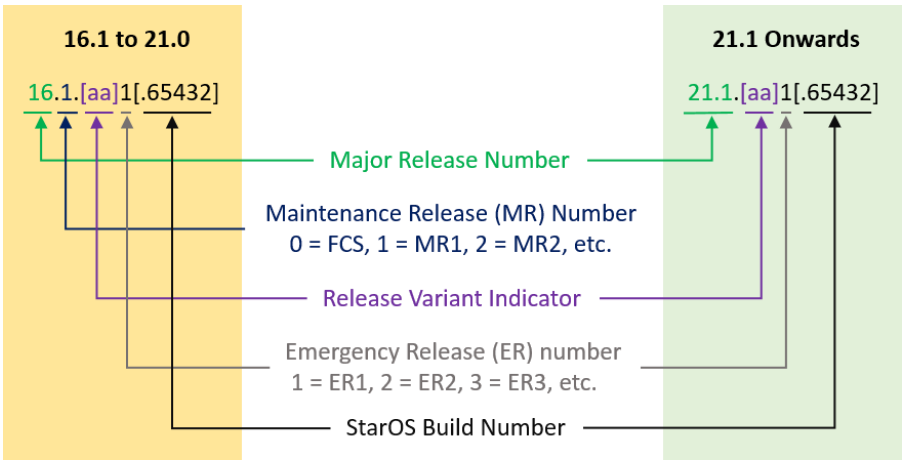
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".



The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".



In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 5 provides descriptions for the packages that are available with this release.

Table 5 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
ASR 5500		
asr5500-<release>.zip	asr5500-<release>.bin	Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T-<release>.zip	asr5500_T-<release>.bin	Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
StarOS Companion Package		
companion-<release>.zip	companion-<release>.tgz	Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants. In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI		
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di-template-vmware-<release>.zip	qvpc-di-template-vmware-<release>.tgz	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-vmware_T-<release>.zip	qvpc-di-template-vmware_T-<release>.tgz	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm-<release>.zip	qvpc-di-template-libvirt-kvm-<release>.tgz	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-template-libvirt-kvm_T-<release>.zip	qvpc-di-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.qcow2.zip	qvpc-di-<release>.qcow2.tgz	Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.qcow2.zip	qvpc-di_T-<release>.qcow2.tgz	Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-SI		
qvpc-si-<release>.bin.zip	qvpc-si-<release>.bin	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.bin.zip	qvpc-si_T-<release>.bin	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 6 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 6 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.
usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm*	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.

* These bundles are also distributed separately from the ISO.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)