Release Notes for StarOS Software Version 21.23.29

First Published: November 05, 2022
Last Updated: November 05, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.23.27. 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	21.23.29, build 87535

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.

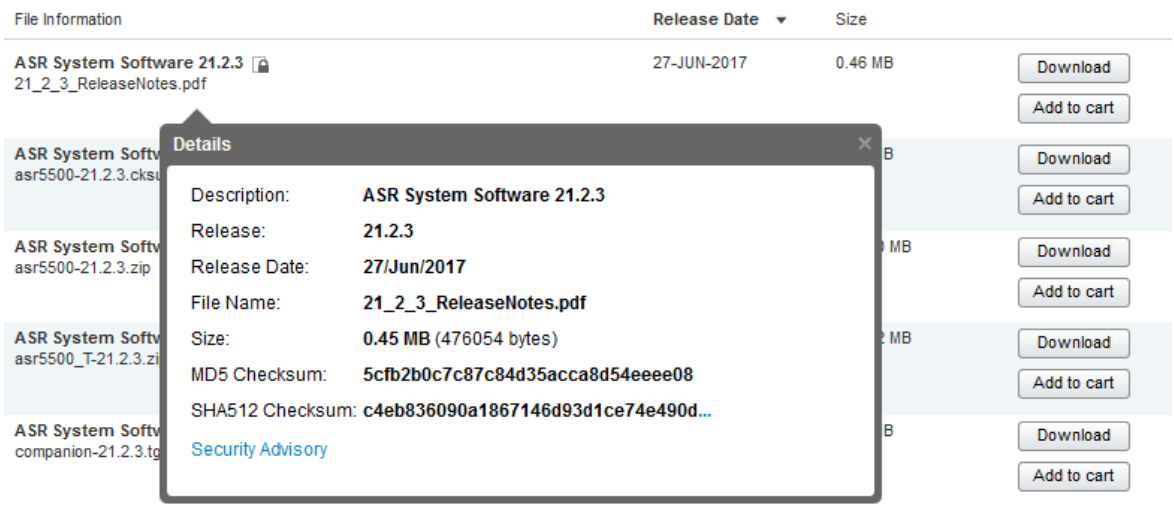
Firmware Updates

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*
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwd19254	[BP-CUPS]:Assertion failure at messenger/memacct.c:539 at Function: sn_memacct_assert_object()	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
CSCwc00980	[CUPS-CP] Task restart at acs_bb_req_cache_alloc()	cups-cp
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running BYT call model	cups-cp
CSCwd37844	[BP-CUPS]Multiple occurrence sessmgr_nlp_gtpu_sess_abort_hndler()sessmgr_nlp_mqueue_timer_handler	cups-cp
CSCvx73208	[BP-CUPS] SessMgr restart at acs_cups_fill_bucket_id_type() while recovering null variable	cups-cp
CSCwc34314	[CUPS UP] Firewall NAT port release behaviour change between legacy and CUPS	cups-cp
CSCwd44023	SGW incorrectly handling collision between MBR &CBR during N26 handover	cups-cp
CSCwb26190	session manager crash at sess/smgr/sessmgr_snx.c	cups-cp
CSCvz46195	sessmgr restart seein in Function: sessmgr_pgw_handle_pcc_intf_evt_modify_rsp()	cups-cp
CSCwb52197	"[CUPS UP] VPP/hatsystem restart clib_memcpy_fast() during IP routes consolidation in BGP, "	cups-up
CSCwb78943	[CUPS] Fatal signal 11 - sess_get_next_pdr_info() - smgr_match_pdr	cups-up
CSCwc54584	[CUPS][npumgr-drv 185001 error vpp_tcp_conn_bind_cb_v6_v4: VPP-LI: Fail to add socket with dhost	cups-up

Bug ID	Headline	Product Found*
CSCvy80968	[BP-CUPS]:[N-1][N-2]Downgraded new standBy UP leads to all call loss once performed UP switchover	cups-up
CSCwc17339	show ssd npu-vpn in UP leaves cli session in unusable state	cups-up
CSCwb07879	LCI/OCI changes CUPS-UP	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCwa46923	CUPS UP sessmgr restart at uplane_decode_tcp_shallow	cups-up
CSCwc55681	CUPS CP Usage Report Failure. Received URR : 0x80000xxx not requested	cups-up
CSCwc63061	sessmgr restart during egtp signalling procedure	cups-up
CSCwd46457	SSD collection may cause BFD timeout with 16 vpp workers due to show memory main-heap	cups-up
CSCwd40057	"After all sessmgr restart, sx-peer-node info is lost on standby chassis"	cups-up
CSCwd16366	LI IPSec tunnel flaps intermittently due to SA Collision	epdg
CSCwc69907	ePDG sessmgr crash on Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:7048	epdg
CSCwa31319	sessmgr restart mme_app_fill_delete_sess_req()	mme
CSCwc65963	sessmgr restart is seen when configuring and unconfiguring Lawful intercept CLIs multiple times	mme
CSCvy33441	sessmgr restart is seen in Function: mme_x2_ho_process_path_sw_req_msg()	mme
CSCwb53675	[MME] release-due-to-pre-emption (39) S1AP radio network cause not implemented	mme
CSCwa36635	MME crashes after upgrade to v21.23.6_21_mme_fsm_event_handler()	mme
CSCwa51122	sessmgr restart seen in Function: egtpc_handle_delete_bearer_rsp_evt()	mme
CSCwc83863	Assertion failure at sess/mme/mme-app/app/mme_app_util.c:18558	mme
CSCwd15146	Additional logging to find reason for S6a notify req with wrong realm	mme
CSCvy67528	[MME Admin guide] Typo in SRVCC config	mme
CSCvz97127	Session manager restart due to an Resource temporarily unavailable on __kernel_vsyscall()	mme
CSCwc43059	sessmgr restart at mme_hss_get_user_data	mme
CSCwc66208	Assertion failure at sess/egtp/egtpc/egtpc_validate_evt.c:1907	mme
CSCwa92153	Corruption in vpnmgr when large amount of data gets dumped	mme
CSCwc51275	Assertion failure at snutil/sn_memblock.c:310 on vMME	mme

Bug ID	Headline	Product Found*
CSCwc59471	sessmgr in warn/over state due to mme_app_allocate_s1nas_msg and SN_cmAlloc()	mme
CSCwa93249	MME sessmgr restart seen in Function: mme_app_egtpc_abort_low_priority_trans()	mme
CSCwa55894	sessmgr restart at egtpc_handle_abort_suspended_proc_cmd_evt	mme
CSCvz90152	SessMgr restart during X2 Handover	mme
CSCwb58470	Clear subscriber not working with service still running	mme
CSCwc80299	"CBC , MME send Write Replace Warning Indication before Write Replace Warning Response"	mme
CSCwb34009	Fatal Signal 11 in acsmgr_destroy_recorded_adc_flows_list()	pdn-gw
CSCwb06949	sessmgr restart on sessmgr_clp_filter function	pdn-gw
CSCvz36326	qci arp-priority-level not updated in config	pdn-gw
CSCwa52583	ICUPS : Session Manager restarts on PGW	pdn-gw
CSCwa59860	Sessmgr crashes after p2p plugin update v2.67.1490	pdn-gw
CSCwc26728	Final cdr with wrong timeOfFirst/LastUsage when “egcdr final-record include-content-ids all”	pdn-gw
CSCwa36871	ADC detection degraded for Youtube	pdn-gw
CSCwa39302	sessmgr crashes sessmgr_rf_fill_service() Assertion failure at sess/smgr/sessmgr_rf.c	pdn-gw
CSCwb81718	CCR-U/CCR-T for Non-WPS session going through WPS channel	pdn-gw
CSCwa50873	Many session disconnect reasons are not documented	pdn-gw
CSCwb23785	Corrupted values of total/output octets displayed in CDR for Ga interface	pdn-gw
CSCwb42809	Nat call object list length going wrong when Insertion failed on NAT call obj list	pdn-gw
CSCwd32146	?Update Bearer Request? is send PGW->SGW without EPS Bearer QoS, which is not aligned with 3GPP	pdn-gw
CSCwa69995	"Duplicated CLI logs with 'user unknown' when CLI is level debug, and grep is being used"	pdn-gw
CSCwd44164	sessmgr task unexpected restarted occurred on PGW acs_http_accel_check	pdn-gw
CSCvx61024	sessmgr restart observed at “sn_ext_process_packet”	pdn-gw
CSCwa52782	Node reloaded after LAG group port reconfiguration	pdn-gw
CSCwc53423	Sessmgr task restart on sess/egtp/egtpc/egtpc_evt_handler_func	pdn-gw
CSCvz70919	RCM OVF deployment for 21.25.x image is not succeeding	rcm
CSCvy05622	Missing documenation on RCM - host-id	rcm

Bug ID	Headline	Product Found*
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCvy86141	Add timeout for NSOSim HTTP POST notification [BEMS01305755]	rcm
CSCwb12055	CLI to prevent multiple config push notifications towards NSO	rcm
CSCvy78942	With WPS3B configuration GW use secondary PAS during mid-session	sae-gw
CSCwa58920	sessmgr process restarted at egtpc_handle_user_sap_event	sae-gw
CSCwa99907	sessmgr process restarted at acsmgr_dcca_send_ccr_terminate()	sae-gw
CSCwa54898	Sessmgr restart - Fatal Signal 6: PC: [09ed1233/X] acsmgr_adc_dispatch_event()	sae-gw
CSCwb55423	[VPC-DI] Sessmgr process restart at sessmgr_pgw_fill_event_record_csr	sae-gw
CSCwa23914	sessmgr restart due Fatal Sig PC: [09fd165b/X] acsmgr_sess_sr_uchkpt_delete_all_accnt_mscc_bucket()	sae-gw
CSCwb58656	sessmgr restart due to Assertion failure at sess/smgr/sessmgr_hlcom.c:467	sae-gw
CSCwb58018	Description of IDFT-support in sgw-service configuration document missing	sae-gw
CSCwd17939	"In sGWRecord, changeTime appearing as before time from recordOpeningTime and duration showing zero"	sae-gw
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvz16012	GMPC event not triggering with reporting action for 3g Detach	sgsn
CSCwc42261	SGW is rejecting the attach even it is emergency apn/subscriber.	sgw
CSCwc95110	[RCM-VM]: Nessus scan vulnerabilities on RCM-VM build 21.23.27 (20220825-090648Z)	smi
CSCvw48686	k8s-ss-mismatch	smi
CSCwb90690	Doc for “show subscribers summary apn 'apn-name' connected-time .... “ to be added	staros
CSCvz94977	Maximum number of NTP servers	staros
CSCwa37867	GRE Tunnel with KA not coming up after Card Migration	staros
CSCwb41992	MACs algorithm configuration does not operate as expected	staros
CSCwd07968	aaamgr going to warn/over state again and again	staros
CSCwc69905	Active/active LAG traffic unbalanced after NPUMGR recovery #02	staros
CSCvy44932	DPC2 card may be marked offline following DDF2 FPGA reporting an error	staros
CSCwa40585	Vpnmgr restart @ vpnmgr_check_addr_conflict()	staros

Bug ID	Headline	Product Found*
CSCwb21297	Sx TX HB Request count not increasing on CNDP DATA UPFs	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*
CSCvy49298	sessmgr task restart at sgwdrv_send_create_session_response()	cups-cp
CSCwc98188	sessmgr crash on CUPS-CP when UE is trying for more than 11 bearers	cups-cp
CSCwc80718	CUPS CP: Memory leak in sn_memblock_cache_alloc_new due to acsmgr_wrap_far_cache	cups-cp
CSCwd29916	IP Pool-ID changes after reload - causing call recovery failures in CP ICSR setup	cups-cp
CSCwd39033	Multiple Sessmgr Crash with function:ipms_flush_hidx	cups-cp
CSCwd40148	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwc97995	[CUPS CP]: WIFI to LTE handoff failure due to EBI mixing with dedicated bearer	cups-cp
CSCwd19115	[BP-CUPS]:Assertion failure at ipms/ipms_api.c:1239 Function: ipms_event()	cups-cp
CSCwc84548	[CPUS-CP] [ICSR] SRP Standby CP sending Sx Session Delete Request which is not expected	cups-cp
CSCwd28140	QER update for AMBR not received by UP from CP	cups-cp
CSCwc87052	Sessmgr gtpu restart at gtpu_sess_abort_handler	cups-cp
CSCwc49447	CP not forwarding PCC dynamic rules to UP over Sx	cups-cp
CSCwd06686	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwc88588	"CUPS-CP - After quota holding timer expiry, CP doesn't invoke Gy"	cups-cp
CSCwc81579	[BP-CUPS] SessMgr restart while processing ICMP packet	cups-up
CSCwc87274	"CUPS,VPP restart in vlan_ip4_qos_mark_node_fn_avx2"	cups-up
CSCwb70785	"CUPS-UP: hatsystem crash due to VPP timeout, Assertion failure at hat/hatsystem_fail.c:2115"	cups-up
CSCwc44211	CUPS UP - Upgrade from 21.23.n9 to 21.23.n10 observed higher RTT/delay between S1U/SGi	cups-up
CSCwd09429	[CUPS] Active ftp is failing - SYN-ACK dropped due to "Invalid TCP pre-connection Request"	cups-up
CSCwd33488	[CUPS UP] Large sx messages retransmission from CP if ipsec is used in Sx	cups-up
CSCwd10956	[BP-CUPS]: Sessmgr crash at uplane_populate_nbr_field_edr_charging_id() after task kill	cups-up

Bug ID	Headline	Product Found*
CSCwd26481	UP not using correct credit-control group config after SO (diameter ignore-service-id option)	cups-up
CSCwb99104	Multiple Sessmgr are in warn state due high memory usage by "epdg_allocate_uli_storage_in_sess" fun	epdg
CSCwc99355	Target MME sending Source SGW IPv6 address in Handover Request	mme
CSCvz46024	[CP-MME] sessmgr restart at egtpc_handle_mod_bearer_cmd_req_evt	mme
CSCwc76543	Multiple frequent sessmgr restart :: mme_app_egtpc_abort_low_priority_trans	mme
CSCwc12610	LicenseExceeded Alarm was not cleared even after subscriber count came below the License limit	mme
CSCwd25108	"DNS Failure - TCP READ, Kernel Closed - req_read_len = 0"	mme
CSCwc80092	Flows are getting terminated even before the configured flow limit is reached	pdn-gw
CSCwc88534	Diagnostic code for unexpected dra peer switch	pdn-gw
CSCwd30690	Ubuntu18.04 LTS / 20.04 LTS / 22.04 LTS : DHCP vulnerabilities (USN-5658-1) seen in 21.23.28 RCM	rcm
CSCwd03984	rcm show-statistics checkpointmgr-session is not working due to ops-center callBack issue	rcm
CSCwc45600	aaamgr restart at aaamgr_gtpp_encode_charging_request	sae-gw
CSCvz41519	DPC 9 card restarted with assert in dcardmgr_update_daddr_dport_handler	staros
CSCvz91284	Traceroute6 fails to immediate next hop	upf
***** Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

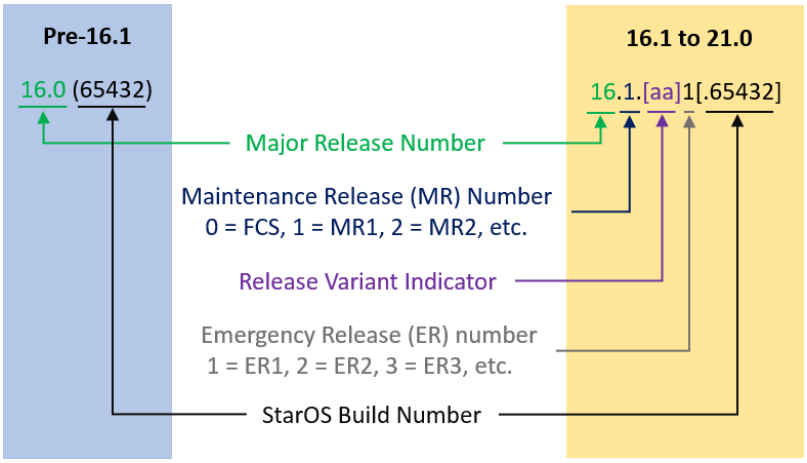
StarOS Version Numbering System

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.

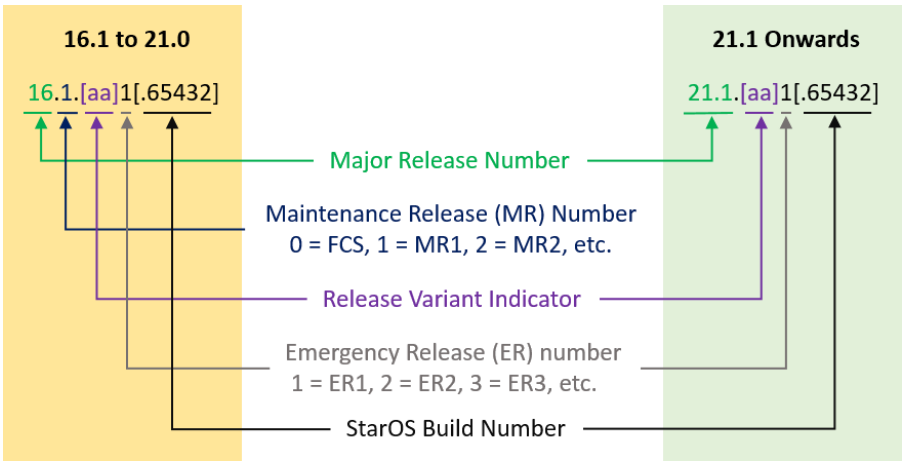
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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