Release Notes for StarOS™ Software Version 21.16.3

First Published: March 16, 2020
Last Updated: Jun 2, 2020

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.16.2. 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	21.16.3, build 74749

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

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 installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

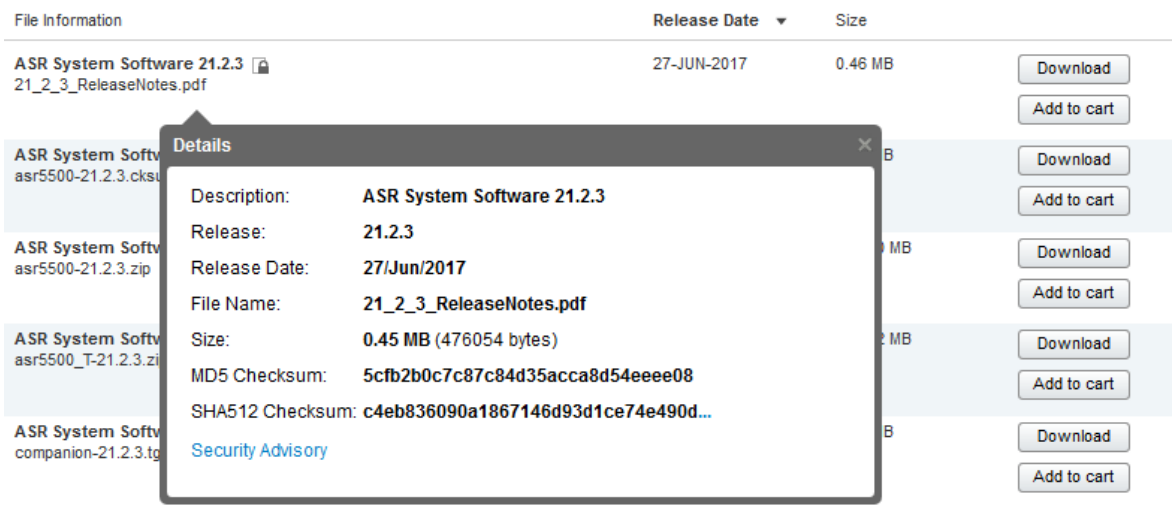
There are no firmware upgrades required for this release.

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 the following mechanisms:

- **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.

- **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

  <product>-<version>.cksums

  Example: asr5500-21.4.0.cksums

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 please see the table below.

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>*

Operating System	SHA512 checksum calculation command examples

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/or that 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*
CSCvr21882	BP CUPS:PC: sgx_update_install_rule_def_list()	cups-cp
CSCvs17393	Multiple Instances of sessmgr restart observed in egtpc_get_ebi_info_from_pdu()	sgsn
CSCvs18939	Multiple Instances of sessmgr restart observed in sgsn_app_allocate_svc_req_cb()	sgsn
CSCvs09909	Routing Area List instance mapping to SRNS cli needs to remove	sgsn
CSCvp05787	sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt()	mme
CSCvr23734	[mme]- congestion-actions triggers not applied during congestion_post reload	mme
CSCvs09989	Cell Whitelist test- UE policy not getting selected for IMEI+MSISDN combination on ASR5500 setup	mme

Bug ID	Headline	Product Found*
CSCvr65974	[BP-ICUPS] MonSub Control packets missing in slowpath generated pcap	pdn-gw
* 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*
CSCvt12235	Some multihop BFD sessions stay in Down state though peer is reachable	staros
CSCvs08833	Cannot save core files larger than 2GB	staros
CSCvs02983	[CUPS]Iftask failurer @ infwdr_msg_pool alloc failure	staros
CSCvs38314	UE's "session time left" and "idle time left" are set to N/A after unplanned migration	staros
CSCvs70898	Active/active LAG traffic unbalanced after NPUMGR recovery	staros
CSCvs09994	sessmgr Segmentation fault in s4_smn_ho_handle_rem_abort	sgsn
CSCvt24677	[TMO] add 3DEC-CBC to cipher list for backward compatiblity on 21.16.dx	cups-cp
CSCvt14477	[sol test] sessmgr task restart with fn: sn_memblock_memcache_free()	cups-up
CSCvt14124	[sol test] sessmgr task restart with fn: sessmgr_sgw_trigger_sx_abort_req()	cups-cp
CSCvr25715	"[BP-CUPS]: [acsmgr 91699 error]:CUPS: Apply Charging Snapshot with key:1, Rulebase: not found."	cups-cp
CSCvs76279	Assertion failure at sess/egtp/egtpc/egtpc_interface.c:258 Function: egtpc_handle_user_sap_event()	cups-cp
CSCvs82607	Current session shows non zero value in sx peers	cups-cp
CSCvs84793	AF sess/sx/sxc/sx_evt_handler_comm.c:608 Function: sx_send_cfm_evt()	cups-cp
CSCvs99539	[BP-CUPS]-sessmgr_uplane_validate_remove_traffic_endpt_sx_sess_modify_req()	cups-up
CSCvs45973	VPP errors - 'no flow found' / 'no free tx slots' on enterprise PGW User plane	cups-up
CSCvt07354	vpp restart in cups-up - Fatal Signal 6: Aborted	cups-up
CSCvs94290	sessmgr assertion failure at sess/egtp/egtpc/egtpc_interface.c:224	cups-cp
CSCvs98253	"SAEGW-UP: sessmgr 12241 error Misc Error3: Clearing call : Sess Report Rsp received with , error cod"	cups-up
CSCvt00492	CUPS-CP : SM crash Fatal Signal 11: Segmentation fault sessmgr_saegw_update_drv_with_sxa_info()	cups-cp
CSCvs55553	Smgr reload sessmgr_uplane_handle_inbound_data_packet sessmgr_egtpu_receive_gtpu_packet uplane_ipv6	cups-up
CSCvs85727	"[TMO] CUPS [fapi 223801 error] Timeout Processing: Time out, MSG ID: 2398, wheel Slot Id: 4, cmd: 5"	cups-up

Bug ID	Headline	Product Found*
CSCvs89945	[BP-CUPS]: Assertion failure at func sessmgr_uplane_gtpu_tx_update	cups-up
CSCvr72750	[CUPS-UP] sessmgr restart - smgr_uplane_create_pdr_from_action_priority()	cups-up
CSCvs59467	vpnmgr restart at vpn_ip_cups_up_retrieve_chunk_info	cups-up
CSCvr05520	[BP-CUPS] sessmgr 10699/ sgw 140014 error- Get Peer Profile Request failed/Failure dispatching event	cups-cp
CSCvs13897	[PLT-CUPS] [fapi 223801 error] fastpath_stream_change_state(); fastpath_stream_modify()	cups-up
CSCvs40711	CUPS: Error Log[acsmgr 91702 error]URR node not found at CP for URR-id	cups-cp
CSCvs59951	"HTTP GET packet doesn't go out of PGW-U plane node on Gi, for specific probe device"	cups-up
CSCvs92102	"[fapi 223801 error] fastpath_stream_delete(): , Hash Delete, seen on all UPs"	cups-up
CSCvs89521	sessmgr crash - segmentation Fault - sessmgr_saegw_update_drv_with_sxa_info	cups-cp
CSCvs49215	NPUMGR restart when U-Plane Node Reloads	cups-up
CSCvs73921	CUPS SGWCDR reporting higher volume traffic comparing with non-CUPS	cups-cp
CSCvq56025	[BP-CUPS] Error log - URR node not found at CP for dedicated bearer on context replacement	cups-cp
CSCvr85577	SRP Last Peer Configuration Error for CDR destination host	cups-cp
CSCvs16287	[TMO CUPS] GTPU discarded packets: Packets Discarded (show gtpu stats)	cups-up
CSCvs55951	[CUPS] Call Summary Log (RTT) for SGW does not include hostname in filename	cups-cp
CSCvs72175	CUPS CP : SM crash Fatal Signal 11: Segmentation fault acsmgr_allocate_cups_sef_info()	cups-cp
CSCvs72199	CUPS CP :PGW-CP node spits continuous log events acsmgr 91699 error CUPS: Charging Snapshot with key	cups-cp
CSCvs72203	CUPS CP: SM crash Assertion failure at sess/smgr/sessmgr_sxu.c:727 sessmgr_sxu_send_release_to_egtpu	cups-cp
CSCvs72236	SM failed due to Assertion failure at sgw_pdn_fsm.c	cups-cp
CSCvn29201	[KT-DVT] only 16 ruledef is displayed "show subscriber user-plane-only-full"	cups-up
CSCvr07640	[BP-CUPS]: Assertion failure at uplane_acsm_compile uplane_build_pattern_matching_automaton	cups-up
CSCvr48845	[UPF-CF] : CF database does not load if chassis is reloaded with saved configuration	cups-up
CSCvs03551	[BP-CUPS] Add new unusual log for mand-ie-incorrect disc-reason	cups-up
CSCvs40366	Potential memory leak issue at function sessmgr_uplane_alloc_simple_buffer	cups-up
CSCvs30808	[BP-CUPS] calls disconnected with reason graceful-cleanup-on-audit-fail after srp switchover	cups-up
CSCvs21549	[BP-CUPS]Discrepency in EDR(sn-ruledef-name) in case flows are terminated by FIN/RST.	cups-up
CSCvs37777	CPU Spike on running Mon Sub on UP.	cups-up
CSCvs64244	audit-gtpumgr-failure CRR Failures observed after SRP Switchover and task restart	cups-up
CSCvr99784	audit-gtpumgr-failure recovery-invalid-crr-clp-uplane-call-info recovery-invalid-crr-clp-uplane-gtpu	cups-up

Bug ID	Headline	Product Found*
CSCvs73630	Fatal Signal 11: 11 PC: [087a4d51/X] egtpc_get_ebi_info_from_pdu()	cups-cp
CSCvr61414	[PLT-CUPS-VPP] capture VPP information when npumgr times out	cups-up
CSCvs03081	Sessmgr restart seen on PGW CP when it receives Sess Report Req	cups-up
CSCvs48422	Cisco CUPS-C restart seen when sending EGTPU release towards U-Plane	cups-cp
CSCvs49774	Cisco CUPS restart seen when Inter-Tech Ho occurs	cups-cp
CSCvs06482	[BP-CUPS] Fatal Signal 6 kernel_vsyscall uplane_populate_url	cups-up
CSCvs15195	[BP-CUPS] Fatal Signal 11: SF PC: [04833da2/X] sessmgr_uplane_apply_action_redirect()	cups-up
CSCvs24627	[BP-CUPS]: Fatal Signal 11 at sessmgr_uplane_action_prioritization	cups-up
CSCvs40189	[BP-CUPS] vpnmgr over memory limits	cups-up
CSCvs53149	Pure-P to Collapsed handover with dedicated bearer triggers corrupted CSRes	cups-cp
CSCvs01291	AssertFail AllocateFromFixedPool() AllocLinkedSharedPoolElem() sx_allocate_tun_node() sx_allocate	cups-up
CSCvs06222	[BP-CUPS]: Series of Assertion failure at sessmgr_egtpu_signalling_routine	cups-up
CSCvs29569	[TMO SOL] Gtpumgr is in over state due to over memory usage on SAEGW-UP	cups-up
CSCvs54487	error indication sent to eNB right after UP SRP switchover	cups-up
CSCvs55556	AssertFail egtpu_process_invalid_evt() egtpu_handle_user_sap_event() sessmgr_uplane_gtpu_tx_setup()	cups-up
CSCvs56180	[CUPS] egtpc_handle_user_sap_event()	cups-cp
CSCvr98233	sgw 140014 error Failure dispatching event <SNX_MSGTYPE_SGW_ADD_PDN_REQ> to SMGR <SN_STATUS_FAILURE>	cups-cp
CSCvs54372	[CUPS] egtpc_handle_user_sap_event()	cups-cp
CSCvs15854	SegFault and Sig6 Abort mspace_malloc() mspace_get_aligned() lookup() _hash_set3() _hash_unset()	cups-up
CSCvs30318	Huge no. of unknown session disconnects observed during longevity	cups-cp
CSCvs51960	Overload Control doesn't work under vpp utilization 100%	cups-up
CSCvs32431	AssertFail: sgwdrv_pdn_fsm_st_disconnecting_evt_clear_pdn() sgwdrv_run_pdn_fsm()	cups-cp
CSCvr84226	[BP-CUPS]-sgwdrv_egtpc_event_dispatch.part.263() __kernel_vsyscall	cups-cp
CSCvs26823	[cups] crash observed @ vpnmgr_srp_cups_up_chunk_msg_recv	cups-up
CSCvr33007	npumgr restart in UP when trying to scale number of VRFs	cups-up
CSCvs26939	[cups] Assertion failure @ snx_sgw_driver_handle_modify_rsp-NTSR	cups-cp
CSCvs32987	VPP CPU "congestion" calculation is broken	cups-up
CSCvs02749	ares_npumgr_vpp_api_reply_handler: Msg reply type 832 not being handled	cups-up
CSCvs33216	[cups] crash observed @ egtpc_handle_user_sap_event -NTSR	cups-cp

Bug ID	Headline	Product Found*
CSCvr98236	"Bad event in sessmgr fsm, event code 8 default call fsm invalid event: state=SMGR_STATE_NEWCALL_ANSW"	cups-cp
CSCvs15581	[BP-CUPS] pgw_drv_fsm_handle_drop_call_in_si_delete_pending	cups-cp
CSCvr98248	"CUPS: sessmgr 10699 error Misc Error: SGW Sx Delete request failed:, error code 1"	cups-cp
CSCvr99655	[CUPS] Shallow Parsing failed with PFCP error cause - Invalid Length (StatsResponse)	cups-cp
CSCvs21309	[CUPS] Session does not delete even if session hold timer expires while NTSR.	cups-cp
CSCvr93913	[BP-CUPS]:Fat Sig 11:sessmgr_saegw_update_drv_with_sxa_info on card migration: huge call-drop	cups-cp
CSCvs25017	[BP-CUPS] asrt @ sess/smgr/sessmgr_sx_util.c:1628 smc_sx_deallocate_pdn_sx_data on standby sae-gw-cp	cups-cp
CSCvr38053	[BP-CUPS] Seg. fault at acsmgr_icsr_frwk_retry_gr_common_send()	cups-cp
CSCvr66345	AssertFail egtpu_get_session() egtpu_handle_user_sap_event() sessmgr_uplane_gtpu_tx_setup()	cups-up
CSCvr97250	[CUPS] fatal crash seen @ snx_fast_buf_alloc	cups-up
CSCvs05052	[BP-CUPS] sm restart at egtpc_recover_sess_from_pdn_rcvry_info()	cups-cp
CSCvr93523	VPP SegFault: clib_memcpy_fast() ip6_frag_do_fragment() smp_egress_extended_ip6_process()	cups-up
CSCvr76635	[BP CUPS] pgw_drv_fsm_handle_modify_bearer_rsp()	cups-cp
CSCvs06591	[BP-CUPS]- sgwdrv_store_clp_pdn_from_egtpc()	cups-cp
CSCvs03367	DIAMETER_PENDING_TRANSACTION is sent as normal Result-Code	sae-gw
CSCvr37080	" [BP-ICUPS]:clib_socket_init: connect (fd 3, '/run/vpp/cli.sock'): Connection refused error"	sae-gw
CSCvs77831	[PLT-ICUPS] vpp restart during callmodel run on ER build	pdn-gw
CSCvs79077	[PLT-ICUPS]: vpp restart during callmodel run on ER build 74218	pdn-gw
CSCvs12083	"[BP-ICUPS] vpp, npumgr,hatsyste,bfdls reload observed in certain conditions when mon-sub is enabled"	pdn-gw
CSCvs07535	[BP-ICUPS] : Monsub activation issue observed for collapsed campon calls intermittently	pdn-gw
***** Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

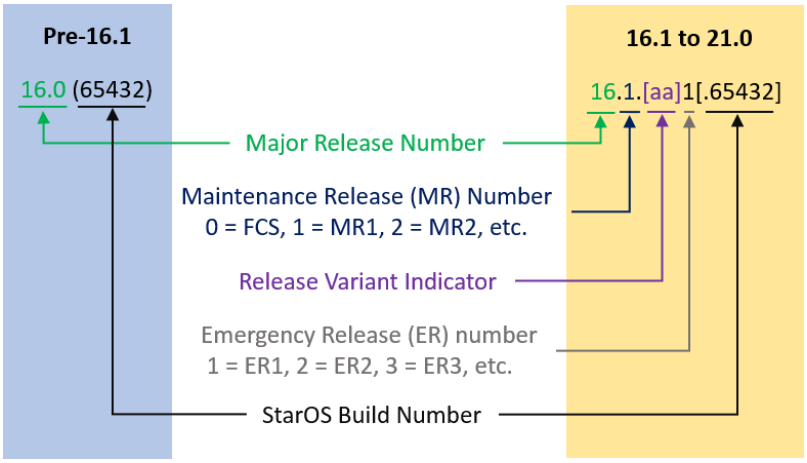
StarOS Version Numbering System

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.

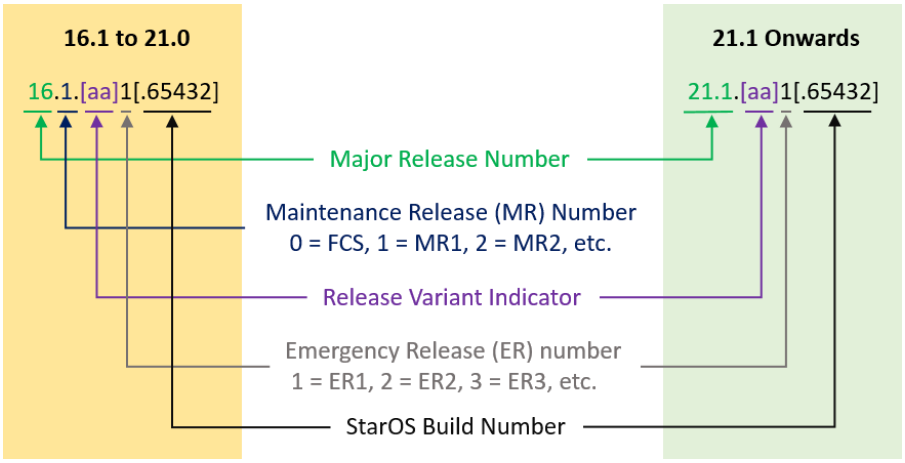
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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

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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
VPC Companion Package		

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

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.