Release Notes for StarOS™ Software Version 21.23.n10

First Published: June 07, 2022
Last Updated: June 07, 2022

Introduction

This Release Note identifies changes and issues related to this software release. These Release Notes identify changes and issues based on 21.23.n9

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.23.n10, build 85656

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

Feature and Behavior Changes

Please contact the Account team for the documentation related to 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

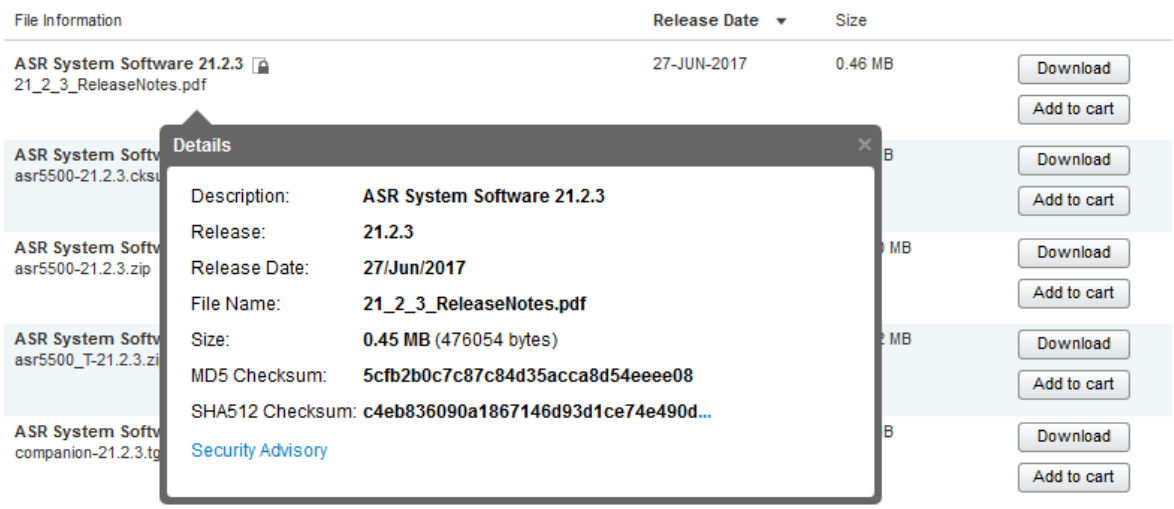
There are no firmware upgrades required for this release.

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*
CSCwc06575	[BP-CUPS]Packet drop in PTT limited pass for CC-group change through Gy(RB change)	cups-up
CSCwc07936	CUPS “pending-traffic-treatment quota-exhausted pass” is not working after back to back pfd push	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	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
CSCwb45809	CUPS: sessmgr restart in sn_slist_comp_xheader_field	cups-up
CSCwb95179	[BP-CUPS] CUTO library is Uninitialized	cups-up

Bug ID	Headline	Product Found*
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up
CSCwb87382	[BP-CUPS]: AF at Func: sn_memblock_cache_get_mcblock_by_addr()	cups-up
CSCwa33605	[CUPS] Error logs DNS snooping: unexpectedly p_hentry is NULL observed (even after fix in 21.23.11)	cups-up
CSCwa92902	[BP-CUPS] Assertion failure at PC: [f67cb491/X] libc.so.6/__memcmp_sse4_2()	cups-up
CSCwa36635	MME crashes after upgrade to v21.23.6_21_mme_fsm_event_handler()	mme
CSCvy33441	sessmgr restart is seen in Function: mme_x2_ho_process_path_sw_req_msg()	mme
CSCwa93249	MME sessmgr restart seen in Function: mme_app_egtpc_abort_low_priority_trans()	mme
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCwa92153	Corruption in vpnmgr when large amount of data gets dumped	mme
CSCvz90152	SessMgr restart during X2 Handover	mme
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCwb12055	CLI to prevent multiple config push notifications towards NSO	rcm
CSCwa64779	RCM HA failing after controller restart	rcm
CSCwa58920	sessmgr process restarted at egtpc_handle_user_sap_event	sae-gw
CSCwa54898	Sessmgr restart - Fatal Signal 6: PC: [09ed1233/X] acsmgr_adc_dispatch_event()	sae-gw
CSCwa23914	sessmgr restart due Fatal Sig PC: [09fd165b/X] acsmgr_sess_sr_uchkpt_delete_all_accnt_mscc_bucket()	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
CSCwa40585	Vpnmgr restart @ vpnmgr_check_addr_conflict()	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*
CSCwb65661	[CUPS] Fatal signal 6 - sgwdrv_process_egtpc_change_notification_ind	cups-cp
CSCvy50239	Incorrect number of the active subscriber in show saegw-service statistics	cups-cp

Bug ID	Headline	Product Found*
CSCwa14260	"active counter for pure-S is still remained , though call is already purged due to sx-path-failure "	cups-cp
CSCwb80543	CUPS CP sessmgr restart at smgr_fsm_state_connected()	cups-cp
CSCwb38173	[BP-CUPS]sessmgr 10396 errors on standby CP.	cups-cp
CSCwb85916	CUPS-CP: Assertion failure at sess/smgr/sessmgr_snx.c:4645	cups-cp
CSCwb56846	[CUPS] data-from/touser-average (APN bulkstat) is still increasing with SGW traffic	cups-cp
CSCvz20360	[BP-CUPS] Observed sessmgr are in warn state after 12 hrs run and with only 5k sessions in system	cups-cp
CSCwb69920	FHT is disappeared after removing diameter host-select table from ims-auth-service config	cups-cp
CSCwb71157	PGW U-addr and SGW U addr for dedicated bearer should be IPv4 if it is created with IPv4 address	cups-cp
CSCwb33013	Random CRBN/RG mismatch in CDRs	cups-cp
CSCwa37735	[CUPS]: 'cc-profile any prepaid-prohibited' cli configured under APN is failing in CUPS setup	cups-cp
CSCwa41564	[BP-CUPS] Current “NAT IP” not cleared post call clear and NBR expiry	cups-cp
CSCwb39582	[CUPS CP] Monitoring key_CP is not reporting the final usage reporting in SX modify response to GX	cups-cp
CSCwb32201	CUPS CP imsa_handle_sgx_delete_notify_callback	cups-cp
CSCwb41424	CUPS CP sessmgr task restart smc_sx_copy_sef_pdu_to_sx_pdu	cups-cp
CSCwb44877	sessmgr Assertion failure at sess/egtp/egtpc/egtpc_interface.c:246	cups-cp
CSCwb42432	[BP-CUPS]: Fatal Signal 11: 11 PC: [03c4aea6/X] sessmgr_pcc_intf_free_cached_sef_evt()	cups-cp
CSCwb35130	"CUPS CP : call-waiting service after the PGW <>GGSN handover , kills volte session"	cups-cp
CSCwb02037	CUPS CP : SGW sess current counter show abnormal increase after ICSR switchover	cups-cp
CSCwa29010	[BP-CUPS] “show config error” does not show errors.	cups-cp
CSCwa86579	Observing sessmgr crash on CP | ggsnapp_process_snx_abort_sub_sess()	cups-cp
CSCvx75520	Observing continuous 'gtpp 52056 warning' logs	cups-cp
CSCwb23375	"CP sends SX PFD messages, despite 'sx-pfd-push disabled' being configured under the user-plane-group"	cups-cp
CSCwb34440	Observing sessmgr crash::sessmgr_sgw_handle_get_peer_profile	cups-cp
CSCwa82550	[CUPS-CP] Discrepancy between Gy and Gz reporting when	cups-cp
CSCwb07947	sessmgr crash | sessmgr_app_svr_event_control_dispatch()	cups-cp
CSCwb36835	sessmgr 11176 error: Unhandled Sx Modify Response in Connected state	cups-cp
CSCwb06340	[CUPS] SGW does not always properly handle release access bearer with 2 sessions	cups-cp
CSCwb16706	[CUPS] sn_assert() egtpc_handle_rel_access_bearers_rsp_evt() egtpc_handle_user_sap_event()	cups-cp
CSCwb05811	[BP-CUPS]Data browsing impacted due to URR mismatch between cp/up.	cups-up
CSCwb22363	CUPS UP stuck ICMP NAT port chunks during TOPUP(rulebase change) 21.23.19	cups-up

Bug ID	Headline	Product Found*
CSCwb54746	Sessmgr restarted on UP at uplane_check_modify_copy_orig_ip_packet()	cups-up
CSCwa59721	[CUPS UP] - Bandwidth Policy not applied after UP Reload	cups-up
CSCwa61829	"APN MTU value isn't applied at UP when push config is disabled,"	cups-up
CSCvz51704	[BP-CUPS]: Segmentation fault at VPP	cups-up
CSCwa18164	Counter rolls over frequently due to inappropriate data-type (e.g. sgw-datastat-dl-qci8totbyte)	cups-up
CSCwa49462	[BP-CUPS] Observed Smgr restart "libc.so.6/__memset_sse2_rep" in Longevity setup	cups-up
CSCwb38623	[BP-CUPS] Observed smgr restart "sessmgr_uplane_process_sx_sess_modify_remove_gx_alias_pdr_list"	cups-up
CSCwb25436	[CUPS UP] sm restart at uplane_update_packet_stats_chunk()	cups-up
CSCwb43121	sessmgr restart at sessmgr_cancel_uplane_dns_query_and_continue	cups-up
CSCwa16073	F124010: L2 traffic steering instance redundancy issue	cups-up
CSCwa98318	[BP-CUPS] Assertion failure at Function: sn_memblock_memcache_alloc()	cups-up
CSCwb27606	[CUPS-UP]Crash at sx_tun_fsm_handle_sess_mod_rsp_evt	cups-up
CSCvz70927	Multiple vpp crashes with 21.25.0.82232	cups-up
CSCwa87274	[UPF] Sessmgr crash : uplane_sfw_nat64_translate_ipv6_to_ipv4 during call running model	cups-up
CSCwb32296	Assertion failure at messenger/mempool.c:399	mme
CSCwa75059	Li packets not getting intercepted when configured with ipv6 src address	mme
CSCwa83203	Observing sessmgr restart::sessmgr_egtpu_receive_gtpu_v6_packet	pdn-gw
CSCwa79949	[soltest]: M6 UPF Sessmgr instances stuck in SERVER Mode after SWO	rcm
CSCwb59156	Assertion failure at acs_copy_to_rule_defn()	sae-gw
CSCwa73707	ssh server config 'client-alive-countmax' is not working	staros
CSCwb26977	Enable VPP full core in non-trusted build	staros
CSCvy31013	DNS queries not leaving the chassis in certain situations	staros
CSCvz28910	Supporting 25G link speed in staros linux kernel code for drivers(i40evf)	staros
CSCwb35998	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf

***** Information in the "Product Found" column identifies the product in which the bug was initially identified.

Operator Notes

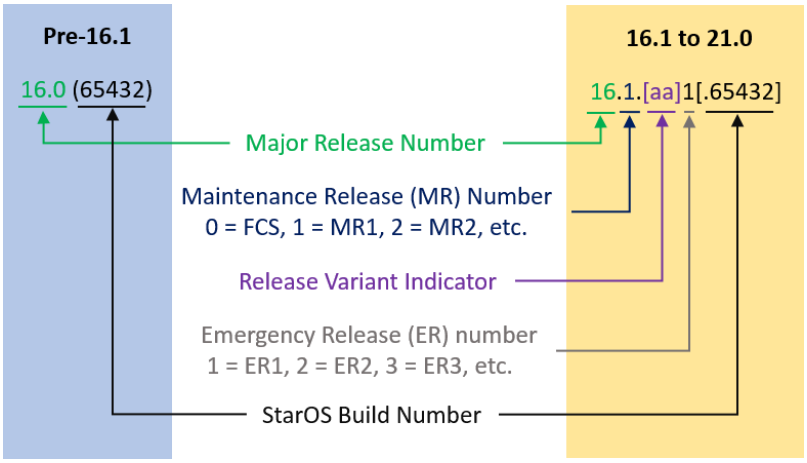
StarOS Version Numbering System

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.

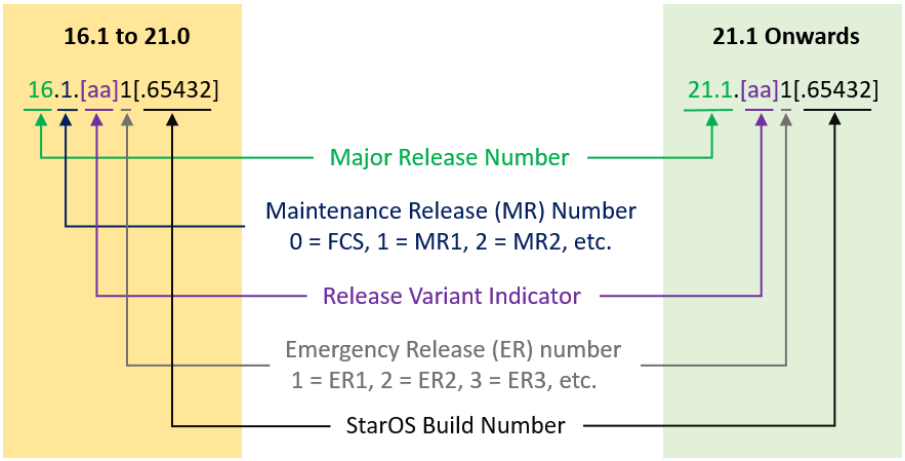
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build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

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.