Release Notes for StarOS™ Software Version 21.23.n8

First Published: February 08, 2022
Last Updated: February 08, 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.n7

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.23.n8, build 83960

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

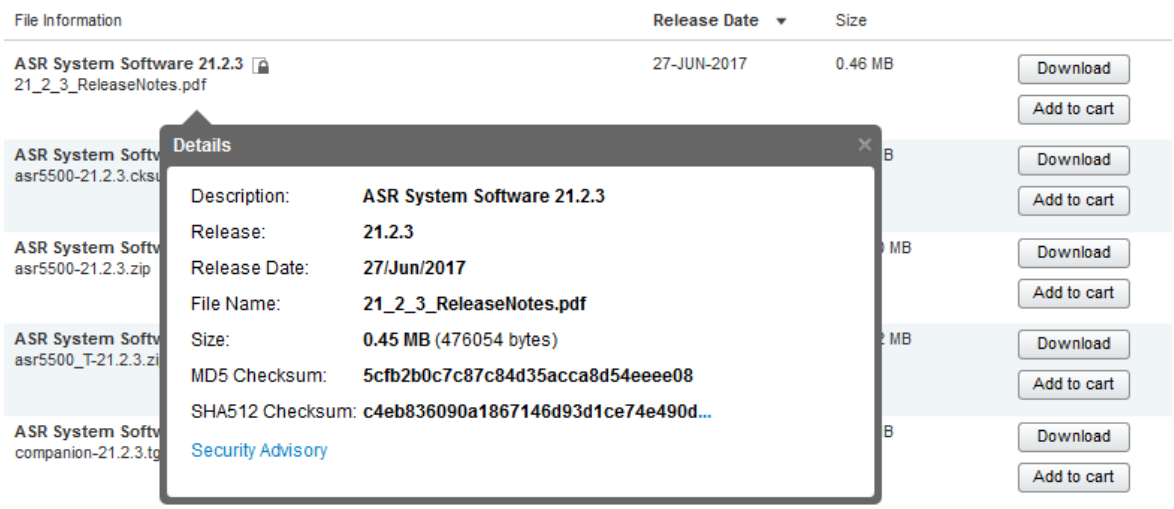
There are no firmware upgrades required for this release.

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*
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running BYT call model	cups-cp
CSCvz66300	[BP-CUPS]: Huge number of session disconnection observed related to sx	cups-cp
CSCwa61799	[CUPS] 4G->2G/3G->4G HO failures - double traffic endpoint deletion	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
CSCwa41564	[BP-CUPS] Current “NAT IP” not cleared post call clear and NBR expiry	cups-cp
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up

Bug ID	Headline	Product Found*
CSCwa38971	[CUPS] PSF - Config “firewall icmp-fsm” block some ICMP responses expected (sollicited)	cups-up
CSCwa33605	[CUPS] Error logs DNS snooping: unexpectedly p_hentry is NULL observed (even after fix in 21.23.11)	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
* 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*
CSCwa51514	[CUPS] PGW should activate “start of traffic” event trigger when OCS grants 0 bytes	cups-cp
CSCwa53617	[CUPS CP] CP is not sending Update QER during 3G UPC (HLR initiated Qos change)	cups-cp
CSCwa75114	Cache not cleared when association of all UPs	cups-cp
CSCwa56879	Fatal 11 at sessmgr_sgw_send_sx_modify_req_trgr_mbreq_init_attach	cups-cp
CSCvz68141	CUPS rejecting sessions instead of disconnecting in out-of-credit prepaid scenario	cups-cp
CSCwa56054	Complete Fix for Monitoring time chekpointing Issues	cups-cp
CSCwa55153	[CUPS CP] “discard-traffic” option inside CCFH Template not working as expected for IPv6	cups-cp
CSCwa33471	Sess mgr restart: Assertion failure at pgw_interface Function: pgw_drv_handle_events_from_smgr	cups-cp
CSCwa38828	[BP-CUPS] Assertion failure @ sx_tun_fsm_handle_sess_del_req_evt	cups-cp
CSCwa40089	[CUPS] Assertion failure Function: smc_sxa_pdn_fsm_handle_sm_rsp_trgr_mbreq_init_attach	cups-cp
CSCwa47719	Fatal Signal 11: 11 PC: [0927f5e2/X] acsmgr_dcca_message_cb()	cups-cp
CSCvz58375	[CUPS CP] “discard-traffic” CLI not supported inside Failure Handling Template	cups-cp
CSCvz95734	[CUPS CP] Collision scenario 4G UBR and CSR for WIFI handoff	cups-cp
CSCwa46766	Crash at PC: [0a454b63/X] acsmgr_dcca_process_msccs()	cups-cp
CSCwa22035	“mSTimeZone” and “servingNodePLMNIdentifie” fields are missing when using GTPP dictonary custom 24	cups-cp
CSCwa37818	CUPS: LI Duplicate Flag visible in show subs	cups-cp
CSCwa05413	CUPS CP - GGSN-C - Unexpected UPC request after HO to 3G of 2 PDN's to the same APN	cups-cp
CSCwa00451	[BP-CUPS] Speed remains at 472 kbps after 2G->4G HO	cups-cp

Bug ID	Headline	Product Found*
CSCwa17341	[BP-CUPS]:Sxdemux crashed at function sn_memblock_memcache_alloc() which resulted in session loss	cups-cp
CSCvz77713	CUPS CP CDR records with recordOpeningTime in future	cups-cp
CSCwa07182	[CUPS CP]After session recovery CP is not shairing Validy Time (time quota) to UP	cups-cp
CSCvz73838	CUPS - CP - High number of snaps acs_handle_events_from_sm_interface()	cups-cp
CSCvz94587	One way traffic broken in CUPS with 4Gto2g(CSFB)to3Gto4G handover	cups-cp
CSCvz86033	[BP-CUPS] chunk withdrawal does not work for ipv4 pool when hold timer is used	cups-cp
CSCvz78239	CUPS CP SM restart at acsmgr_allocate_cups_sef_info()	cups-cp
CSCwa41897	[CUPS] APN bulkstat data-touseravg-pps and data-fromuseravg-bps are counting SGW traffic	cups-up
CSCwa72377	Multiple crashes with UP reboot	cups-up
CSCwa68973	Memory Leak Leading to Sessmgr Restarts in CUPS	cups-up
CSCwa22111	[CUPS UP] sessmgr restart is seen in function uplane_update_packet_stats_chunk()	cups-up
CSCvz62621	Fatal Signal 11: 11 in PC: [04d9a45d/X] uplane_analyze_udp()	cups-up
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up
CSCvz76372	N-3: sessctrl assert @sctrl_cfg_sync_decode_traffic_optimization_profile_config_tlv()	cups-up
CSCvz52524	[BP-CUPS] Observed Function: sxdatamgr_delete_all_cc_group_in_a_service() During UP De-Registration	cups-up
CSCvz97499	Sessmgr stuck in SERVER mode	cups-up
CSCwa59048	Multiple crashes in CUPS-CP nodes	cups-up
CSCwa48477	Few attribute not capturing values or missing values in EDRs - user-location-information	cups-up
CSCvy67623	[BP-CUPS] gtpu disconnects reported as remote-disconnect at UP	cups-up
CSCvz50778	CUPS UP - Packets stuck in VPP queue under unknown conditions	cups-up
CSCvz98048	[CUPS UP] - Bulk statistics file contains only 50 rulebases for rulebase schema	cups-up
CSCwa22158	CUPS UP - Fatal signal 11 in uplane_create_app_data_flow	cups-up
CSCwa29657	[CUPS-UP] SessMgr restart on uplane_adf_init_l4()	cups-up
CSCwa21101	vpp restart in vlan_ip4_qos_mark_node_fn_avx2()	cups-up
CSCwa34741	Downlink traffic not matching ruledef for dedicated bearer	cups-up
CSCvz91900	Fatal Signal 11 - Segmentation Fault at VPP	cups-up
CSCwa23655	CUPS CP Sending “AN_GW_Failed” in absence of Ruledef in Rulebase	cups-up
CSCvz92880	vpp thread/memif mapping issue after (double) sessmgr restart	cups-up
CSCvz83471	CUPS-UP - Traffic is hitting only single VPP thread - IPV6 RSS may not work on non Intel NIC	cups-up
CSCvz70975	CUPS UP NBR records missing charging-id and other fields	cups-up

Bug ID	Headline	Product Found*
CSCvz52115	cli no ikev2-ikesa **dh-group** reuse is incorrectly getting saved in config	epdg
CSCvt53343	sessmgr restart at mme_abort_pdn_disconnect_procedure()	mme
CSCvt59071	Assertion Failure for function mme_app_fill_dnlink_data_notification_failure_ind()	mme
CSCvw81248	Abnormal high counter values in MME tai schema counters after upgrade	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvx68053	sessmgr Segmentation fault at mme_app_remove_pdn_from_pgwlist()	mme
CSCvy89382	WRITE-REPLACE WARNING RESPONSE messages not received by MME after enabling WRWI	mme
CSCvz71291	Abnormal values of tai schema counters	mme
CSCvz80074	MME function mme_pdn_connect_cbr_ind_awt_csr() Crash	mme
CSCvw96092	session manager restarts at pgw_drv_clear_drv_clp_due_to_gngp_ctxt_replacement	pdn-gw
CSCwa35893	VPC-SI | 21.23.6 | Build 81507 | Node reload after npumgr failure ares_npumgr_process_gre_tun_nh	pdn-gw
CSCvx96693	VPP buffer leak when “drops due to interna 1973” is seen	pdn-gw
CSCvw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCwa12377	sessctrl restart on standby after reboot	pdn-gw
CSCvx66315	Duplicate charging id seen during ICSR upgrade scenario	pdn-gw
CSCvz22700	SSD cli process reloads with show diameter route table debug-info	sae-gw
CSCvx78219	remove mme peer command is not working as expected	sgsn
CSCvx87351	“ODB roamerAccessToVPLMN-AP-Barred” set in ISD in 3G RAU/4G-3G Handovers not working properly	sgsn
CSCwa37651	SGW CDR not containing all RANSecondaryRATUsageReport - underbilling	sgw
CSCvz96864	CAF2 reports false CAF_CRC_FAILURE/CAFPRGERR	staros
CSCwa60130	[UPF]Uplink stream in preactive state leading to packets stuck in vpp.	upf
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

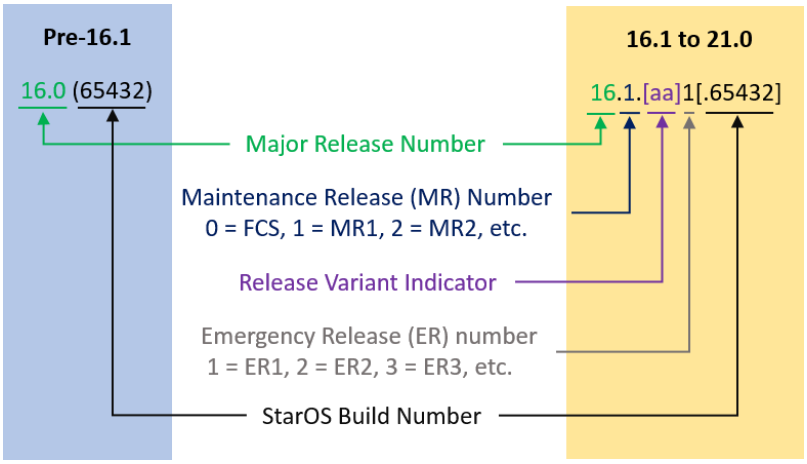
StarOS Version Numbering System

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.

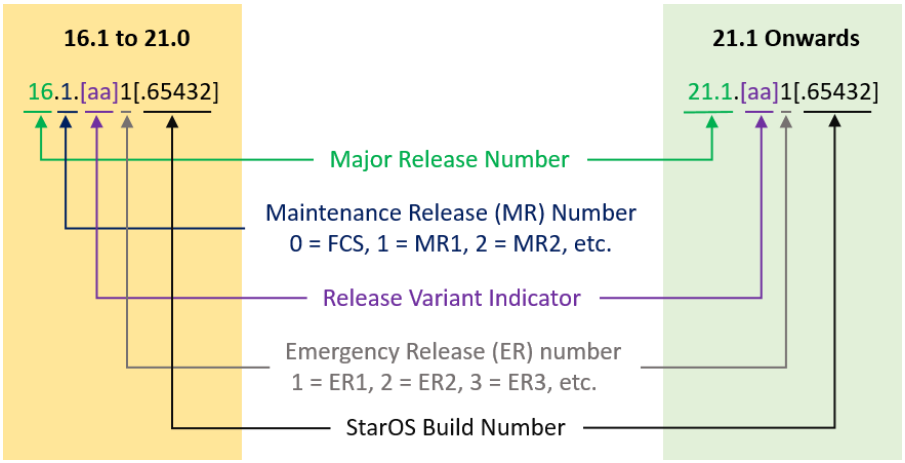
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build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

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

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