Release Notes for StarOS™ Software Version 21.20.5

First Published: Sept 30, 2020
Last Updated: Sept 30, 2020

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.20.4. 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	21.20.5, build 77667

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

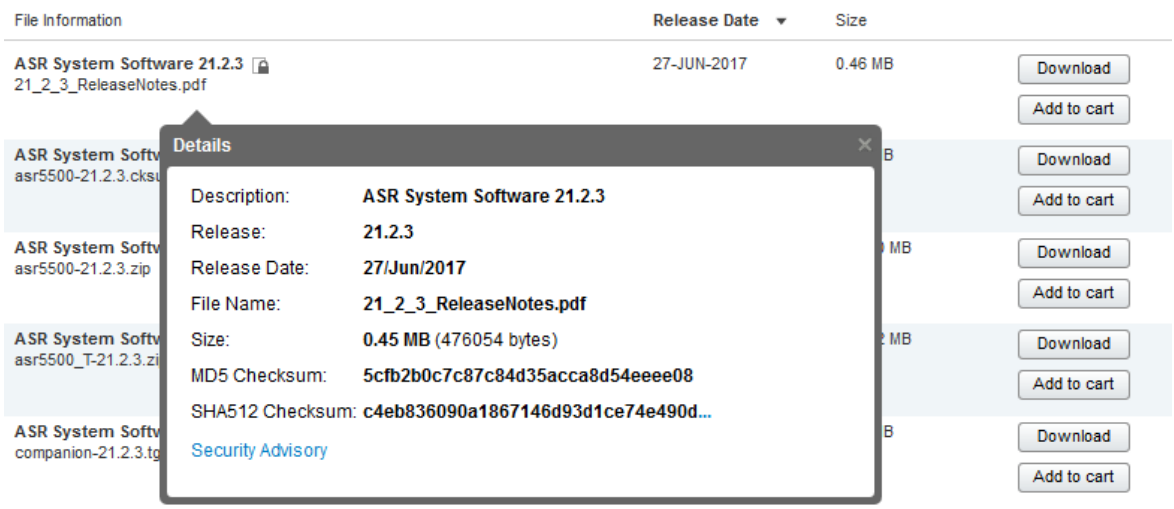
There are no firmware upgrades required for this release.

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*
CSCvu82215	[acsmgr 91699 error] : CUPS: FindUrr URR ID returned mismatch for ACS_BUCKET_TYPE_GY	cups-cp
CSCvu36637	vpn 5013 error - #012Alloc request received from invalid up-id 0 up-grp-name UP-GROUP-1	cups-cp
CSCvv39677	CP: all vpnmgr instances in memory over state	cups-cp
CSCvv10225	CP:SX Report requests - denied or not responded after unplanned active SF migration - compute reboot	cups-cp
CSCvu29628	sx-path-failure observed while performed active box reload	cups-cp
CSCvt46570	[BP-CUPS]: Huge checkpoint failure at Standby micro-checkpoint failures recovery record not found	cups-cp

Bug ID	Headline	Product Found*
CSCvt73405	[BP:CUPS]: [acsmgr 91702 error]URR node not found at CP for URR-id: 0x779	cups-cp
CSCvu33117	BP-CUPS-acsmgr_free_cups_sef_info()	cups-cp
CSCvu96189	"[BP-CUPS] After CP ICSR, USU is not encoded if there was no GSU for the MSCC"	cups-cp
CSCvv03378	"[BP-CUPS]: 12241: sessmgr_ggsn_fill_sub_sess_recovery_info: sgsn gtpu addr NULL callid 99c0d4,"	cups-cp
CSCvu45618	[BP-CUPS] huge number of session disconnects with reason sxfail-opr-get-usagereport	cups-cp
CSCvv89085	Call loss is seen with failure reason user-plane-info-not-available during call model run	cups-cp
CSCvv54870	FUI-Terminate reporting to Gx-PCRF	cups-cp
CSCvv50922	2 QERs sent by CP for 3G/2G GGSN Calls	cups-cp
CSCvv77051	Bearer Context Shallow Parsing failed - message seen during Pure-S Dedicated Bearer S1-Handover	cups-cp
CSCvv58459	"[RCM] Sx peering status always shows Push in Progress from CP, when pfd-push is disabled"	cups-up
CSCvv05853	CRR recovery failures - audit-npumgr-failure and audit-vpnmgr-failure	cups-up
CSCvv52658	[RCM] UP reboot didn't switchover to Stby. Instead RCM kept rebooting UPs(Act and Stby) cyclically	cups-up
CSCvv62933	[RCM] UP unable to register to RCM even though RCM VIP is reachable	cups-up
CSCvv56994	[RCM] 2 Active PGW UP's reboot did not lead to Standby coming up for 1 Active UP	cups-up
CSCvu38266	"[fapi 223801 error] fastpath_stream_delete(): Hash Delete, returned error 0x80005004"	cups-up
CSCvv87105	"Bulkstat crash: Fatal Signal 6: 6, PC: [f67ec12a/X] libc.so.6/__memset_sse2_rep()"	mme
CSCvv19288	MME: few Optional IEs need to be added / updated in messages over N26 interface	mme
CSCvq14634	Bogus PDN statistics observed at MME	mme
CSCvv89000	PDN Connectivity procedure and ERAB Modification Indication procedure MBR collision	mme
CSCvv55758	[CP-MME]- Multiple Sessmgr task went in to warn state on Longevity more than 72hr	mme
CSCvu80679	MME doesn't handle the Exp Result Code 5511 when received from IWK-SCEF in CIA message	mme
CSCvu82139	[CP-MME]- Post unplanned card failure diamproxy/diactrl instances went to over state	mme
CSCvu65266	Assertion failure while configuring Diameter destination realm under mme-service with context MME	mme
CSCvu81466	[MONTE Roaming] On VPC-DI while doing mmemgr restart seen 18K subs drop from total 1.4M	mme
CSCvu37233	On VPC-DI Multiple Sessmgr restarts seen while doing SF card migration from active to standby	mme
CSCvv36310	IP Bad checksum with Rewrite TTL on Downlink Packets feature	pdn-gw

Bug ID	Headline	Product Found*
CSCvu14360	[DPC2] Around 7% sessmgr card cpu 5min degradation observed in Tethering feature wrt Baseline	pdn-gw
CSCvv90960	[PLT-ICUPS] : Order of fragmented packets being changed by ASR5500	pdn-gw
CSCvv82186	[BP-ICUPS]: one HSLI server did not get removed even tho config removed from chassis	pdn-gw
CSCvu36991	BP-ICUPS : Existing flows/throughput impacted when new flows/calls are made	pdn-gw
CSCvv86188	[BP-ICUPS]: TCP conn proxy/ LI TCP connections did not come up after ICSR	pdn-gw
CSCvv69285	[BP-ICUPS]: difference in intercepted call stats in 2 LI commands	pdn-gw
CSCvv45493	[BP-ICUPS]: Interception of UL/Dl packets is not happening for Rule Based Gx-LI Dynamic Rule	sae-gw
CSCvv59404	vSGW UP resiliency not working when integrated with RCM	rcm
CSCvv60086	"[RCM] RCM Ops Center config not committing, HTTP 500 Internal Server Error"	rcm
CSCvu99478	Health check parameter is not applied correctly from AutoVNF to ESC	usp-uas
CSCvu18110	Confdmgr process has restarted in MME	usp-usf
CSCvv10506	Confdmgr process has restarted in MME	usp-usf
CSCvv08382	UEM restarts occur when the command show deployment-vnfr: vnfrs vnfr deployment-name is executed	usp-usf
* 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*
CSCvu06329	[CUPS-DI-CP] [CEPS] CEPS case for Ultra platform taking too high iftask utilization	cups-cp
CSCvv41572	URR ID not synchronized CP and UP after server un-reachable condition	cups-cp
CSCvv37834	Missing ULI in Update Bearer Response in 21.20.3.76888	cups-cp
CSCvu74458	UP Selection Failure No Service Group Available after SF migration on CP	cups-cp
CSCvv33067	gtpumgr and vpnmgr take time to restart when demux migrated due to DIMM ECC Error detected.	cups-cp
CSCvu87741	CP installs a new FAR for Redirect every time a RAR comes from Gy	cups-cp
CSCvv66489	HTTP Flows inside the Flow-EDRs have incorrect Ruledef-Name	cups-cp
CSCvv64787	CP ignoring Sx-Estab-Response with no-resources-available	cups-cp

Bug ID	Headline	Product Found*
CSCvv58832	Radius Accounting message sent twice for RAT-Trigger	cups-cp
CSCvs40215	[BP-CUPS] resultCode IE missing in CDR in CUPS	cups-cp
CSCvv68494	[CUPS] Discrepancy in vpp cpu utilization calculation	cups-up
CSCvv15236	DDN: sessmgr restart with sessmgr_uplane_prepare_and_send_end_marker_pkt()	cups-up
CSCvt14477	[sol test] sessmgr task restart with fn: sn_memblock_memcache_free()	cups-up
CSCvu93220	CUPS P2P Statistics are not adding up	cups-up
CSCvu66665	Static Gz URR not created on UserPlane post reboot	cups-up
CSCvu97888	Allow TCP Handshake packets to flow without rulematch (Delay Charging)	cups-up
CSCvu00189	APN bulkstats UL/DL packets and bytes counter values not matching.	cups-up
CSCvv59651	ICMP Flows have incorrect SN-APP-Protocol in EDRs	cups-up
CSCvu72509	[BP-CUPS]: 'SX_SESSION_REPORT_REQUEST' is sent multiple times for the GyURR with FAR	cups-up
CSCvv04526	CUPS/RCM SRP switchover failure : Geographic-Redundancy can not preinstall call	cups-up
CSCvp46985	[PLT-CUPS-VPP]:Retransmissions are wrongly getting counted for data having OOO packets	cups-up
CSCvu29089	E-RAB Modification Indication collision scenario with Create Bearer response	mme
CSCvv20352	[PLT-ICUPS] npumgr restart at dh_api_get_sockets_handler	pdn-gw
CSCvv52504	PGW not setting the IPv6 Layer Hop Limit	pdn-gw
CSCvt29099	[PLT-ICUPS]:Multi protocol flows are not optimized by CUTO	pdn-gw
CSCvv48487	[BP-ICUPS]Heartbeat interval is not updated with min 1 tcp connection	pdn-gw
CSCvv55485	[BP-ICUPS]: increment in the FAC VPP Connections Share Limit Exceeded counter for legacy CUSP	pdn-gw
CSCvv64850	[BP-ICUPS] APN-AMBR value not passing to CUTO Lib for Default Non-GBR Bearer	pdn-gw
CSCvv64960	[BP-ICUPS] APN-MBR value is applied to the UDP flow even though dynamic rule MBR value is lower.	pdn-gw
CSCvv72642	[BP-ICUPS] MBR value is 0 in TODR for MBR/GBR Extended rates in Legacy for CUTO	pdn-gw
CSCvv13604	[BP-ICUPS]: show lawful-intercept full all output not updated immedeatily for Gx Rule Intercept UDP	sae-gw
CSCvv50926	Rollback not done in other nodes when management connectivity lost to one node	staros
CSCvv51372	Script does not retry connection after timeout during filesystem synchronize	staros
CSCvv27931	Add enterprise fails with large number of IP Pools	staros
CSCvu99445	UPF is accepting calls even if license is expired	upf
CSCvv01962	"Oakla UL packet Drops, User Plane Function (UPF)"	upf

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

Operator Notes

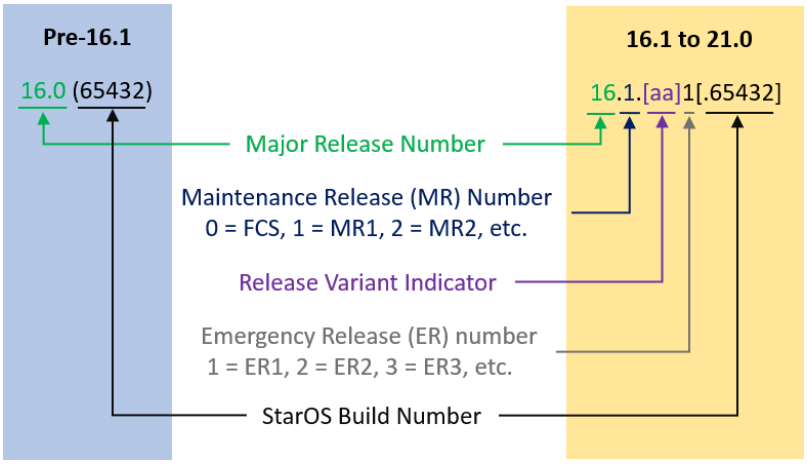
StarOS Version Numbering System

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

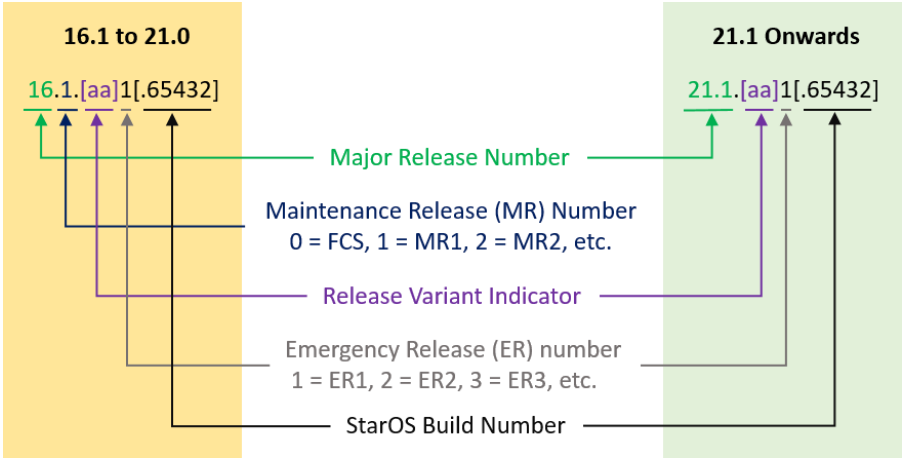
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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

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



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



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

Release Package Descriptions

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

Table 5 - Release Package Information

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

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