



Release Notes for StarOS™ Software Version 21.15.3

First Published: September 30, 2019

Last Updated: September 30, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.15.2. 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	21.15.3, build 73070

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

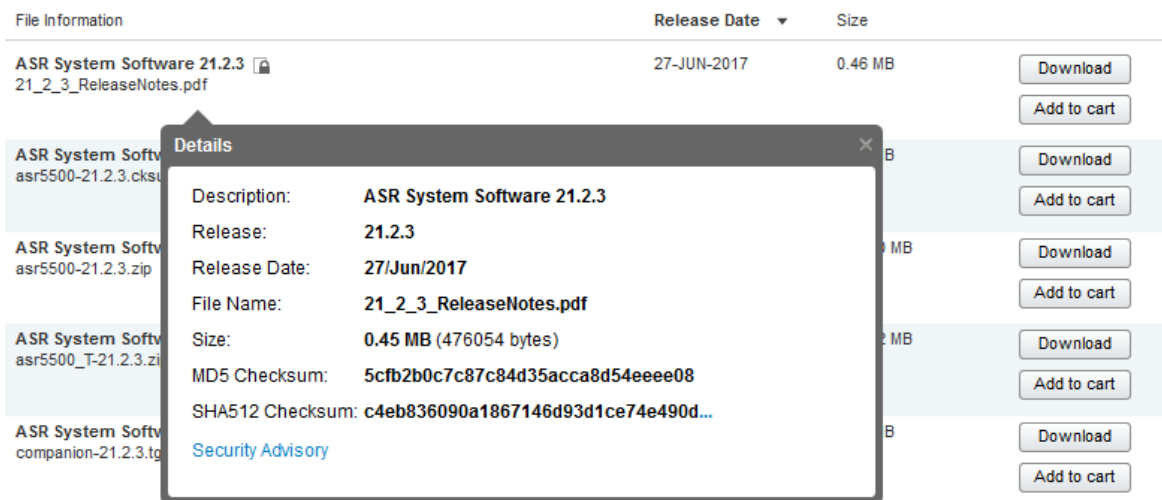
There are no firmware upgrades required for this release.

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 <pre>> certutil.exe -hashfile <filename>.<extension> SHA512</pre>
Apple MAC	Open a terminal window and type the following command <pre>\$ shasum -a 512 <filename>.<extension></pre>

Open Bugs in this Release

Operating System	SHA512 checksum calculation command examples
Linux	Open a terminal window and type the following command <pre>\$ sha512sum <filename>.<extension></pre> Or <pre>\$ shasum -a 512 <filename>.<extension></pre>
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*
CSCvo33959	[PLT-CUPS]:vpnmgr restart observed on CP when UP is reloaded during planned upgrade.	cups-cp
CSCvq18230	"[BP-CUPS]: Call not preallocated to standby chassis, when more than 2 dedicated bearers are created"	cups-cp
CSCvq90677	[BP-CUPS]: Calls dropped on other UPs on bringing down a UP from UP group	cups-cp
CSCvm61038	[BP-CUPS] Call drop with "sx-no-response" in UP after ICSR Switchover	cups-cp
CSCvm61615	[BP-CUPS] Dynamic rule charging is not there when Rulebase changes(disable to enable egcdr).	cups-cp

Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvn05051	[BP-CUPS]: series of sessmgr 11703 error logs while sending ftp traffic	cups-cp
CSCvn08050	[BP-CUPS] CLI "monitor peer bfd install-delay 60" install-delay command can't be removed	cups-cp
CSCvn43321	CUPS: CCR-U and CCR-T doesn't follow the diameter pending timeout configuration	cups-cp
CSCvo45414	sx-invalid-response seen when dynamic rule installed after predefined rule and sesMgr kill	cups-cp
CSCvo87689	[BP-CUPS] Quota info not sent on SX when received in Gy CCA-I	cups-cp
CSCvp99905	"[BP-CUPS]: post PtoC SGW HO, on call clear SX MODIFY request is rejected for ipv4v6 call"	cups-cp
CSCvq00003	"[BP-CUPS-VPP]:Rulebase name not getting updated in sessions full o/p and in CDR,after RB change"	cups-cp
CSCvq13842	[CUPS-CP] sxdemux task does not recover after unplanned SF failure.	cups-cp
CSCvq18084	[BP-CUPS]- acsmgr error URR-SeqNum received(2) is smaller than existing(3)	cups-cp
CSCvq27786	[BP-CUPS] acsmgr_allocate_cups_ses_params()	cups-cp
CSCvq35037	[BP-CUPS]:acsmgr_fill_urr_count()	cups-cp
CSCvq35047	"[BP-CUPS]:[BP-CUPS]:SGW Sx Abort request failed:, error code 1"	cups-cp
CSCvq44831	[BP-CUPS]- sessmgr_collect_sgw_call_rcvry_info()	cups-cp
CSCvq53786	sxfail-opr-revert-info session disconnects seen on CP	cups-cp
CSCvq91130	[BP-CUPS] npumgrs on SFs in warn state for cputime	cups-cp
CSCvq94578	[BP-CUPS]-Invalid/unhandled PDN event <SGWDRV_PDN_EVT_S1_ERROR_IND>	cups-cp
CSCvr04110	[GGSN]- sessmgr_pgw_find_sx_trans_info_node()	cups-cp
CSCvr09016	[BP-CUPS]- acsmgr_mgr_cups_api.c:13420 Charging Snapshot with key not found on any of the bearers	cups-cp
CSCvr19250	BP CUPS: SegFault sn_memblock_cache_block_flush()	cups-cp
CSCvr19841	BP CUPS: sessmgr_egtpu_send_error_indication()	cups-cp
CSCvr20193	BP CUPS: sessmgr 11091 sessmgr_sx_util.c: driver and sessmgr are out of sync - Internal Error. ebi 7	cups-cp
CSCvr21616	BP CUPS:PC: [f67ca71f/X] libc.so.6/___strncpy_sse2()	cups-cp
CSCvr21750	BP CUPS:sx_tun_fsm_handle_sess_estab_rsp_msg()	cups-cp
CSCvr21882	BP CUPS:PC: sgx_update_install_rule_def_list()	cups-cp
CSCvr27266	[BP CUPS] sgwdrv_epsb_fsm_st_connecting_evt_s1u_status()	cups-cp

Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvr29572	[BP CUPS] sessmgr_pgw_clean_pcc_trans_node_in_app_info()	cups-cp
CSCvr32557	"[BP-CUPS]: Call not coming up, when installing 64 rules on default bearer after reload"	cups-cp
CSCvr35282	[CUPS] Bulkstat task face Nonfatal warning at messenger/xpt_tcp.c:1030	cups-cp
CSCvr46462	CUPS: SM fail due to Segmentation fault on sessmgr_uplane_periodic_process_urr_queue	cups-cp
CSCvm73084	[BP-CUPS]: Pure-S call fails at the UP with unknown reason	cups-cp
CSCvo13831	[BP-CUPS] Second PDR not displayed for ADC rule in show active-charging session full	cups-cp
CSCvo21126	Sx Session Establishment Request encoding issues	cups-cp
CSCvo35511	[BP-CUPS] mon pro PFD compression flag needs to be enabled for respective IEs	cups-cp
CSCvo46856	[BP-CUPS]: SxModiReq/res counter remains 0 in sx-service statistics	cups-cp
CSCvp35114	"[BP-CUPS] SX_Session_Est_Resp recived with SEID as 0, still call is accepted"	cups-cp
CSCvp81541	CUPS/SX Out Header Creation invalid format	cups-cp
CSCvr10741	"HD-RAID volume is not overwriting old files after reaching over 92% capacity full, and missing CDRs."	cups-cp
CSCvp59415	[BP-CUPS] sx_allocate_trans_rec()	cups-up
CSCvq17827	[CUPS] UP rejects SX_SESSION_ESTABLISHMENT_REQUEST after sessmgr crash	cups-up
CSCvr21675	[PLT-CUPS] VPP SegFault - fastpath_3tuple_ip4_node_fn() fastpath_6tuple_ip4_node_fn()	cups-up
CSCvk75614	[BP-CUPS] START TIME/END TIME IE is not getting populated except Sx deletion response message.	cups-up
CSCvn14202	[BP-CUPS-VPP]Delay charging is having issues with Tear Down packets.	cups-up
CSCvn35496	Sessmgr assertion at function fastpath_stream_add_internal_inline()	cups-up
CSCvn35513	[BP-CUPS-VPP]: Sessmgr Assertion failure at ../../buildscache/vpp/41/	cups-up
CSCvn40163	[BP-CUPS-VPP]: Basic collapsed Sx call - input data packets dropped	cups-up
CSCvn50204	[PLT -CUPS-VPP] License exceeded notification in UP when the state of license is good	cups-up
CSCvn52966	"[BP-CUPS]:Total TCP Pkts/bytes, FP Pkts/bytes in TCP analyser stats dont count discarded packets"	cups-up
CSCvn60293	flow-add-failed count is increased while make and break call is running	cups-up
CSCvn68360	[BP-CUPS]: HTTP flow is marked as error when L7 analyser is enabled	cups-up

Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvn85404	[BP-CUPS] : Packet filter list at Uplane is getting corrupted resulting in incorrect rule match	cups-up
CSCvn93223	[CUPS]TRM stats are not shown on User Plane	cups-up
CSCvo01375	[CUPS] VPP restart observed with stack libvlib.so.0/unix_cli_file_welcome_timer()	cups-up
CSCvo07207	[BP-CUPS] sessctrl restart in UP	cups-up
CSCvo14095	[BP-CUPS] Sessctrl is in Over state when there is no activity on the UP	cups-up
CSCvo39232	[PLT-CUPS] memif packet drops observed with single call running HTTP traffic	cups-up
CSCvp39466	[CUPS] row read failures observed on both UPs during CM run	cups-up
CSCvp47022	[BP-CUPS] : PACKET MEASUREMENTis not sent in radius URR and hence not shown in accounting-msg	cups-up
CSCvp84112	[BP-CUPS]:Issue with SGW handover for Pure P call with DSCP marking enabled and QOS changes	cups-up
CSCvq35024	sessmgr error: Misc Error:Callline invalid or in invalid state for sending checkpoints	cups-up
CSCvq64442	Subscriber pkt drop stats not updated to sessmgr from VPP on call clear.	cups-up
CSCvq67869	ULI attribute is not correct in EDR when ECGL is sent in ULI after UP ICSR Switchover.	cups-up
CSCvq71873	sessmgr_uplane_cleanup_pdr()	cups-up
CSCvq87098	[UPF-SVI] QOS not being applied evenly across all calls with static rulebase	cups-up
CSCvq88630	Error- urr Rule Chkpt not exist - urr_element deletion failed	cups-up
CSCvq90988	[PLT-CUPS-VPP] Sig 6 abort at /usr/sbin64/vpp(sn_assert_signal_handler()+0x11b9)	cups-up
CSCvr21683	BP CUPS:free_acct()	cups-up
CSCvr38739	Need to create multiple TCP segments if Xheader inserted packet size is > MSS	cups-up
CSCvm01940	"[BP-CUPS-VPP] Packets are counted in charging, though packets are dropped in vpp."	cups-up
CSCvm05260	[BP-CUPS] Incorrect starttime and duration measurement when no data is sent post recalculate measure	cups-up
CSCvm39163	[BP-CUPS-VPP]IP flow readdressing is not working correctly when mid flow readdressing is applied.	cups-up
CSCvm47700	[BP-CUPS-VPP]: cli: show user-plane-service statistics analyzer name http has corrupted data	cups-up
CSCvo22723	[CUPS]DL Volume bytes does not match in show subs user-plane and Sx_session_delete_response in X2 HO	cups-up

Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvo29502	[BP-CUPS]:Gz & Gy URR is not getting created for a predef rule installed on default bearer with VoGx	cups-up
CSCvo45567	[BP-CUPS] START TIME is zero in Sx Deletion response for Gz bearer level URR.	cups-up
CSCvo47244	[BP-CUPS] Discrepancy in dropped packet count statistics after Gy quota exhausted	cups-up
CSCvo68451	[CUPS]Multiple sessmgr restart observed on UP while performing CRP test case	cups-up
CSCvp46985	[PLT-CUPS-VPP]:Retransmissions are wrongly getting counted for data having OOO packets	cups-up
CSCvr16004	[BP-CUPS] : First dL pkt is getting forwarded when the flow action is discard in CA.	cups-up
CSCvr08929	sessmgr restart seen on mme_app_fill_delete_sess_req	mme
CSCvq03879	Single-registration-indication flag not set in case of 4G->3G->4G PS-HO	mme
CSCvq93693	MME config update not happening on reload chasis applying enb-goup config	mme
CSCvr49046	[PLT-ICUPS-VPP] Bundle rotation issue observed for high data rate traffic	pdn-gw
CSCvn55676	[BP-CUPS]:Uplink Stream remain in Config state after Flow status change	pdn-gw
CSCvr40741	PLT-ICUPS : vppctl show errors incrementing “lookup drops” and “PAWS check failed”	pdn-gw
CSCvr43201	PLT-ICUPS :CUTO Flows are not cleared up in VPP after sessmgr restart	pdn-gw
CSCvr43208	PLT-ICUPS : npu utilization is very high with HS UE	pdn-gw
CSCvr46799	[PLT-ICUPS] : With full VPP 4G and 5G LI is not working	pdn-gw
CSCvr48112	[BP-ICUPS] : Sessmgr reload is seen while capturing slow path packets capture	pdn-gw
CSCvr48347	BP-ICUPS : Sessmgr restart at acsmgr_data_receive_merge_mode	pdn-gw
CSCvr48351	[BP-ICUPS] : Slowpath pcap file rotation not happening for mon sub feature.	pdn-gw
CSCvr49023	[BP-ICUPS] Pcap files are not retained in expected path for Mon Sub feature.	pdn-gw
CSCvr49030	[BP-ICUPS] Unable to configure monsub Poll timer along with EDR config	pdn-gw
CSCvr49043	[BP-ICUPS] SMGR reload observed when partial pkt size is modified during active mon sub tracing.	pdn-gw
CSCvq95469	[BP-ICUPS-VPP]: icmpv6/mppls-vpnv6 pkts not being delivered to sessmgr.	sae-gw
CSCvq88658	[BP-PLT-CUPS]- iftask_sigusr1_signal_handler()	staros
CSCvr48128	[Mon Sub] Multiple vpp/npu reloads observed during continues tracing	staros
CSCvr40362	UAME - K8S Cluster Node Recovery Actions (Post VM recovery by ESC) - Cluster SYNC fails	usp-uas

* 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*
CSCvr46818	[BP-CUPS] Quota-Hold-Time is NOT working after ICSR on Control-Plane	cups-cp
CSCvr35282	[CUPS] Bulkstat task face Nonfatal warning at messenger/xpt_tcp.c:1030	cups-cp
CSCvr39257	BP CUPS: libc.so.6/___memcpy_ssse3_rep	cups-up
CSCvq90947	IPV6 flow label being reset to 0x0 in iPhone while engaging CUSP Proxy	pdn-gw
CSCvq91157	CUSP enabled chassis reporting connectivity issue while utilizing VPN (443 based - HTTPS)	pdn-gw
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

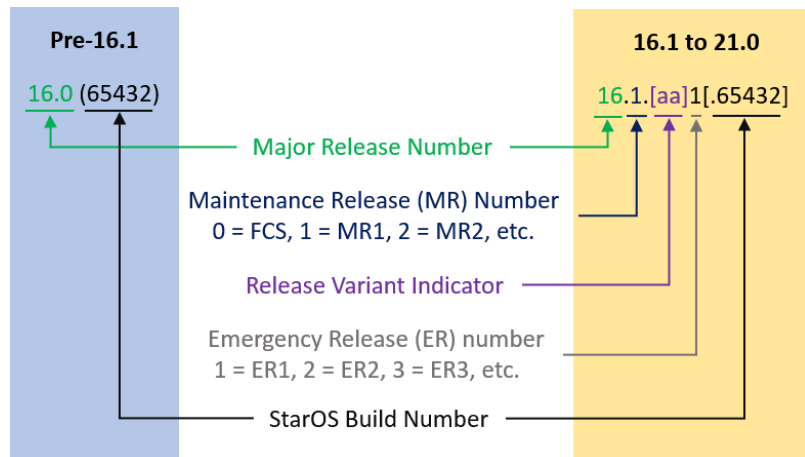
StarOS Version Numbering System

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.

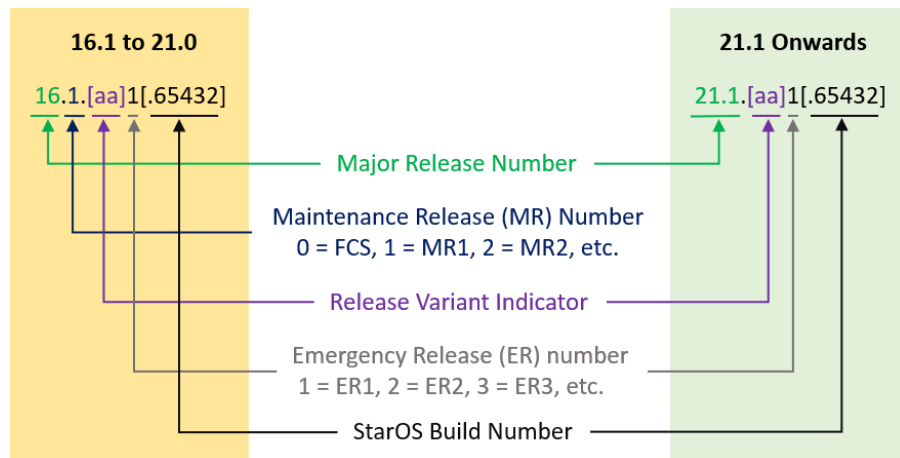
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

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".



Operator Notes

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		

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di- <release>.bin.zip	qvpc-di- <release>.bin	<p>Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>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.</p>
qvpc-di_T- <release>.bin.zip	qvpc-di_T- <release>.bin	<p>Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>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.</p>
qvpc-di- <release>.iso.zip	qvpc-di- <release>.iso	<p>Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>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.</p>
qvpc-di_T- <release>.iso.zip	qvpc-di_T- <release>.iso	<p>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.</p> <p>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.</p>
qvpc-di-template- vmware- <release>.zip	qvpc-di-template- vmware- <release>.tgz	<p>Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>
qvpc-di-template- vmware_T- <release>.zip	qvpc-di-template- vmware_T- <release>.tgz	<p>Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-di-template-libvirt-kvm-<release>.zip	qvmc-di-template-libvirt-kvm-<release>.tgz	<p>Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>
qvmc-di-template-libvirt-kvm_T-<release>.zip	qvmc-di-template-libvirt-kvm_T-<release>.tgz	<p>Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>
qvmc-di-<release>.qcow2.zip	qvmc-di-<release>.qcow2.tgz	<p>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.</p> <p>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.</p>
qvmc-di_T-<release>.qcow2.zip	qvmc-di_T-<release>.qcow2.tgz	<p>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.</p> <p>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.</p>
VPC-SI		
qvmc-si-<release>.bin.zip	qvmc-si-<release>.bin	<p>Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>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.</p>
qvmc-si_T-<release>.bin.zip	qvmc-si_T-<release>.bin	<p>Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>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.</p>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-si- <release>.iso.zip	qvmc-si- <release>.iso	<p>Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>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.</p>
qvmc-si_T- <release>.iso.zip	qvmc-si_T- <release>.iso	<p>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.</p> <p>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.</p>
qvmc-si-template- vmware- <release>.zip	qvmc-si-template- vmware- <release>.ova	<p>Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>
qvmc-si-template- vmware_T- <release>.zip	qvmc-si-template- vmware_T- <release>.ova	<p>Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>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.</p>
qvmc-si-template- libvirt-kvm- <release>.zip	qvmc-si-template- libvirt-kvm- <release>.tgz	<p>Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>
qvmc-si-template- libvirt-kvm_T- <release>.zip	qvmc-si-template- libvirt-kvm_T- <release>.tgz	<p>Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>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.</p>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.