



# Release Notes for StarOS™ Software Version 21.23.b3

**First Published:** October 25, 2021

**Last Updated:** October 25, 2021

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.23.b2. 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	21.23.b3, build 82673

## Feature and Behavior Changes

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

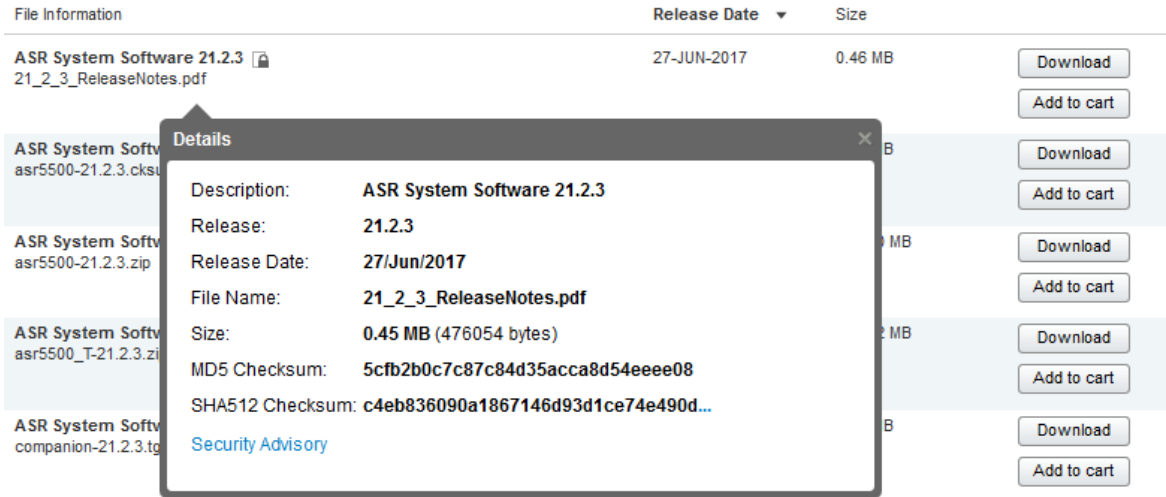
## Firmware Updates

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 **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.

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 see [Table 2](#).

**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>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>
Apple MAC	Open a terminal window and type the following command  <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
Linux	Open a terminal window and type the following command  <pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
<p><b>NOTES:</b></p> <p>&lt;filename&gt; is the name of the file.</p> <p>&lt;extension&gt; is the file extension (e.g. .zip or .tgz).</p>	

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 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*
CSCvz67952	sessmgr restart during PDN releasing connection procedure	cups-cp
CSCvz49537	[CUPS-CP] sessmgr restart is seen at Function: sgwdrv_allow_sm_event_in_assert_hit()	cups-cp
CSCvz38631	[CUPS CP] micro checkpoint failures and sessmgr 10396 error on standby CP	cups-cp
CSCvz00059	CUPS CP SM restart at API sgwdrv_process_egtpc_delete_bearer_ind()	cups-cp
CSCvy87801	[CUPS]memory leak on functions acsmgr_allocate_cups_info() and acsmgr_allocate_cups_sef_info()	cups-cp
CSCvz30638	[BP-CUPS]sessmgr_call_recover_install_sgw_drv_callline_for_collapsed_call()sessmgr_recover_call_pgw	cups-cp
CSCvx45677	[CUPS] [SGWCDR] - Missing "RANSecondaryRATUsageReport" inside SGWCDR	cups-cp
CSCvz12338	[BP-CUPS] UP-GROUP-NAME and UP-NODE-ID o/p not displayed in subs saegw-only all	cups-cp
CSCvw94565	[BP-CUPS] Inconsistency behavior in handling Predefined Rule and Group-of-Ruledef at control plane	cups-cp
CSCvx23431	Less than 16 rules are not working without CLI : no policy-control update-default-bearer	cups-cp
CSCvx78549	[BP-CUPS] Observed restart sessmgr_pgw_fill_pgw_trans_node_from_sx_sef_out_info in Longevity run	cups-cp
CSCvy78249	CCR-U does not have RSU when responding to a RAR	cups-cp
CSCvy63380	CUPS CP Adds Null Value 0.0.0.0 as the servingNodeAddress in PGW-CDR (PERMANENT FIX)	cups-cp
CSCvy79949	CUPS IDFT SGWCDR RecClosingCause	cups-cp
CSCvy78310	FUI-Terminate 4012 issues on CUPS	cups-cp
CSCvy14092	[BP-CUPS] vpnmgr crash at vpnmgr_get_loc_vpn_chunk_details_by_vpnid	cups-cp
CSCvy13010	CP Loses FUI-Redirect info and switches to QRT	cups-cp
CSCvy36038	CUPS CP Adds Null Value 0.0.0.0 as the servingNodeAddress in PGW-CDR	cups-cp
CSCvy34261	[BP-CUPS] VOGX accumulated octects are sent in CCR-U instead of in CCR-T for 3G Call	cups-cp

## Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvz29030	Multiple error logs observed	cups-cp
CSCvz64067	[BP-CUPS] Observed sessmgr restart "sx_tun_fsm_handle_sess_del_req_msg" in Longevity run	cups-up
CSCvz44817	CUPS UP - sessmgr crash in uplane_p2p_update_stats	cups-up
CSCvx32019	"[BP-CUPS] Mid call predefrule changes from rated to free for all components, not charged correctly."	cups-up
CSCvy83173	CUPS UPF rulebase statistics limited to 50 rulebases	cups-up
CSCvz30527	[BP-CUPS]AF at at snutil/sn_memblock.c:310 sn_memblock_memcache_free()uplane_sfw_nat_release_nat_ip	cups-up
CSCvz30533	[BP-CUPS] [1/0/15207 <sessmgr:9> sessmgr_sef.c:14374] NBR Report Validation error Message dropped	cups-up
CSCvw04208	show subscribers user-plane-only callid <id> qos-group statistics not giving correct o/p on v21.x.gx	cups-up
CSCvy57500	[BP-PCT] Incorrect bytes and pkts seen for http analyzer stats.	cups-up
CSCvs23558	[BP-CUPS] PC: [048dd1d7/X] smgr_uplane_handle_config_chrg_action()	cups-up
CSCvu14090	[BP-CUPS] sessmgr restart at add_chunk() function	cups-up
CSCvv79637	"[SNMP]SNMP mib compilation errors seen for starServiceChainName, starUPPlaneTsMissConfig"	cups-up
CSCvw43171	[CUPS] [PFD Management] - Inconsistent rulebase configuration between CP & UP	cups-up
CSCvv27398	Sessmgr not offloading SSL traffic for particular kind of SSL error	cups-up
CSCvw83244	Uplink packet drops after 4g->3G handover on CUPS UP with this error: ADF UL TEID/QFI key mismatch	cups-up
CSCvw91145	Display error in syslog for source ip address violation by IPv4 and IPv6 subscriber	cups-up
CSCvx61691	[UPF-SVI] :sessmgr restart at sessmgr_uplane_free_p2p_session()	cups-up
CSCvx83812	Sessmgr restart on standby UP @smgr_uplane_handle_load_optbldb()	cups-up
CSCvy50850	[BP-CUPS] sessmgr restart "snx_uplane_driver_event_control_dispatch" during Longevity run	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCvu24136	Sessmgr reloaded due to sn_memblock_memcache_free()	cups-up
CSCvy57179	Incorrect MEMIF - BIA mapping in the FIB Table	cups-up
CSCvx32800	[CUPS / UPF-DATA] Fatal Signal 11 at sessmgr_uplane_readdr_adf_compare_hash_entry	cups-up
CSCvx28193	"Sessmgr restart in sn_memblock_memcache_alloc, sxmgr_allocate_pfcpeer_trans_entry on UP ICSR"	cups-up
CSCvz51704	[BP-CUPS]: Segmentation fault at VPP	cups-up
CSCvz44817	CUPS UP - sessmgr crash in uplane_p2p_update_stats	cups-up
CSCvz38208	sessmgr restart @ uplane_cleanup_freed_app_data_flow()	cups-up
CSCvz52114	[BP-CUPS] sessmgr assert @ sn_memblock_memcache_alloc()	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up

## Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvz39850	[BP-CUPS]uplane_sfw_nat_allocate_port_chunk_from_recovery_list()uplane_sfw_nat_recover_nat_realm_	cups-up
CSCvu81466	Sessmgr restart due to Erab Modification Indication collision with ERAB setup Procedure	mme
CSCvy63363	MME responds with DIAMETER_UNABLE_TO_COMPLY(5012) after receiving IDR with pscsf-restoration bit set	mme
CSCvz29322	Authentcation failures between MME and UE after 3g-4g enablement on RADIO network	mme
CSCvz39725	DCN id is incorrectly sent in ATTACH ACCEPT	mme
CSCvz22259	sessmgr restart seen in function egtpc_validate_modify_bearer_req_evt()	mme
CSCvz26204	NR restriction flag is lost after sessmgr restart	mme
CSCvy61494	multi fault with sessmgr restart Function: mme_app_fill_s1_bearer_values()	mme
CSCvy81424	X2 Handover does not work due to possible incorrect NextHop in PathSwitchReqAck	mme
CSCvy86561	Month parameter wrongly encoded by MME and sent to GMPC server	mme
CSCvw94840	assert observed on func "S1apMD_handle_peercfg_rtrv_rsp()"	mme
CSCvy31118	MME should reject duplicate eNB IDs	mme
CSCvq68326	mme_mgr restart is seen in mme_mgr_aggregate_msg_to_sessmgr()	mme
CSCvw13552	Echo req seen for gtp peers even when echo is not configured in MME.	mme
CSCvy42092	Assertion failure during MME offload: Assertion failure at sess/mme/mme-app/app/mme_app_smgr.c:380	mme
CSCvy90143	Auto recovery for "Failed to send Diameter Message" issue	mme
CSCvy14226	[CP-MME] Session manager restart at mme_pdn_disconnect_complete	mme
CSCvy02339	Parameters are encoded wrongly at MME and sent to GMPC server	mme
CSCvy02388	MME rejects Service Request with unknown EMM cause after back-to-back sessmgr restart	mme
CSCvy24493	TrackingAreaUpdate causes dedicated bearer release with cause invalid-qos-combination	mme
CSCvy14531	Multiple SESSMGRs in WARN/OVER state	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvu81466	Sessmgr restart due to Erab Modification Indication collision with ERAB setup Procedure	mme
CSCvz82295	BP-ICUPS: sm crashes at acsmgr_fp_get_gy_quota	pdn-gw
CSCvz38569	BP-ICUPS : Incorrect reporting of Time-First-Usage AVP in the RF records	pdn-gw
CSCvx57389	UE port not written in QCI1 CDR for Vowifi call	pdn-gw
CSCvs65289	[BP-ICUPS]:Policer row not created in one direction for accelerated flow	pdn-gw
CSCvy13275	show lawful-intercept imei returns No matching LI session/trigger found with active data session	pdn-gw

## Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCVy30776	Wrong CDRs are generated by PGW on receiving Secondary RAT Usage Reports in CNR	pdn-gw
CSCVy78471	"[BP-LEGACY]:Rf-SDC does not have CSG info when MBR to enter hyb-sub cell, CCAU send rule trigger CBR"	pdn-gw
CSCVx66200	[BP-ICUPS]:SM crashes observed on active and standby with "acsmgr_deallocate_call_obj()"	pdn-gw
CSCVx79042	Unexpected debug logs are observed during ICSR switchover with L2TP subscribers	pdn-gw
CSCVw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCVy02352	Parameters are encoded wrongly at SGSN and sent to GMPC server	sgsn
CSCVx44868	sessmgr restart seen with Function: SmGenSuspendReq	sgsn
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
CSCVz58034	[S8HR-Legacy] BBIFF Intercepted details are cleared on sessmgr recovery	sgw
CSCVz34526	[SGW-S8HR] Extra bytes seen in IMS Signaling/Media Messages	sgw
CSCVz34975	[S8HR LI] Message TLVs Endianness and Format corrections	sgw
CSCVy12988	Wrong CDRs are generated by SGW on receiving Secondary RAT Usage Reports	sgw
CSCVz58034	[S8HR-Legacy] BBIFF Intercepted details are cleared on sessmgr recovery	sgw
CSCVz67912	[S8HR-Legacy] Observed sessmgr crash on ICSR switchover and cli crash on executing S8HR show command	sgw
CSCVx98820	[CUPS-TACACS-IPsec] TCP connection failure with second tacacs server during failover	staros
CSCVw51050	21.14: Port speed OID changes after port up/down	staros
CSCVy63440	Port Tx traffic not balanced across MIO cards	staros
CSCVy16147	"[UPF]Incorrect tos being marked for combo UPF, when charging action has tos and sgw marks inner pkt."	upf
CSCVw15307	Sessmgr restart sessmgr_uplane_match_rule_after_cf	upf
CSCVx02862	"[Combo-UPF]5G-4G handover , UE goes to Idle, D/L data , debuffering, after that all pkts to sessmgr."	upf
CSCVx08150	[UPF-SVI] Assertion at sn_memblock_memcache_alloc() while 5G call-model was running	upf
CSCVx14614	"[Combo-UPF]Per peer statistics are incorrect for combo calls, in multi smf topology."	upf
CSCVx38146	[UPF]:Incosistent behaviour for Change in content-ID not updating TEP row	upf
CSCVx62133	Invalid content filtering policy id assigned to UE and potential sessmgr crash	upf
CSCVx92756	[UPF-SVI]: Sessmgr restarted at uplane_drv_handle_events_from_smgr()	upf
CSCVy18530	UPF : UL ICMP packet is buffered even when UL FAR Action is forward	upf
* 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*
CSCvz25891	[BP-CUPS] Assertion failure @ func sessmgr_sx_sesscount_inform_timeout	cups-up
CSCvx69801	ruledef not getting removed in UP when "no ruledef" is configured and pushed to UP	cups-up

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

## Operator Notes

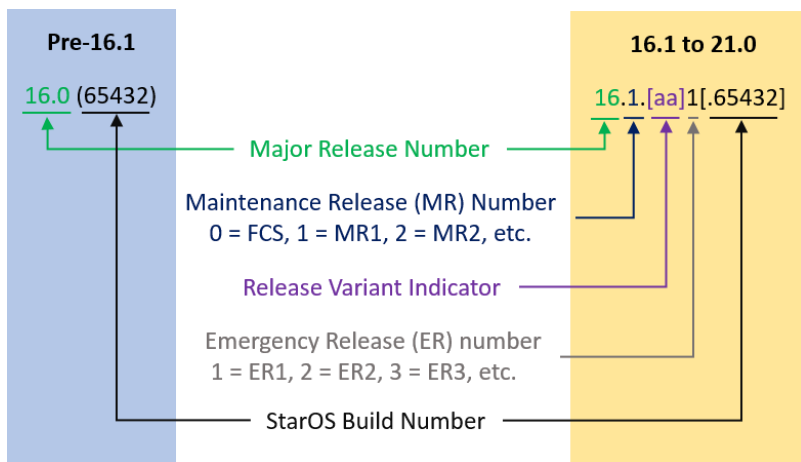
### StarOS Version Numbering System

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.

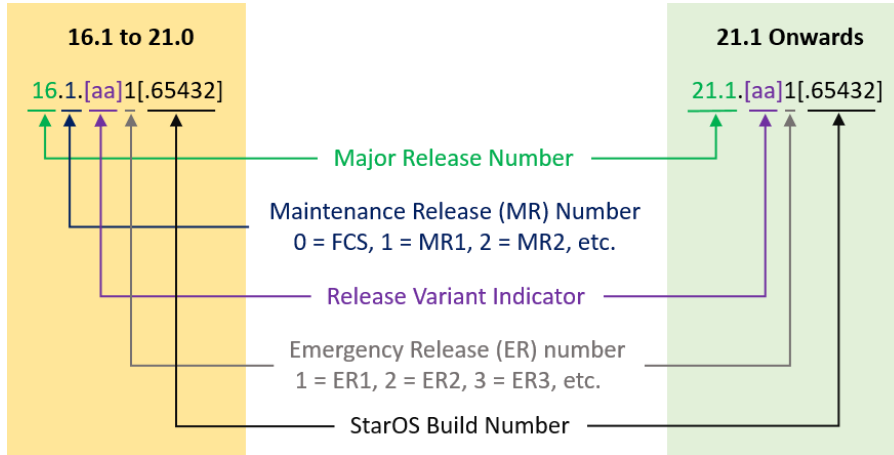
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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
<b>ASR 5500</b>		
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.
<b>StarOS Companion Package</b>		
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.
<b>VPC-DI</b>		
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
qvmc-di-template-vmware-<release>.zip	qvmc-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>
qvmc-di-template-vmware_T-<release>.zip	qvmc-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>
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>
<b>VPC-SI</b>		
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>

## Operator Notes

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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>
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>
qvmc-si-<release>.qcow2.zip	qvmc-si-<release>.qcow2.gz	<p>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.</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_T- <release>.qcow2.zip	qvmc-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.
<b>VPC Companion Package</b>		
companion-vmc- <release>.zip	companion-vmc- <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.
<b>Ultra Service Platform</b>		
usp-<version>.iso		The USP software package containing component RPMs (bundles).  Refer to <a href="#">Table 6</a> for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images.  Refer to <a href="#">Table 6</a> for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

**Table 6 - USP ISO Bundles**

USP Bundle Name	Description
usp-em-bundle-<version>-1.x86_64.rpm*	The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.
usp-ugp-bundle-<version>-1.x86_64.rpm*	The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle.
usp-yang-bundle-<version>-1.x86_64.rpm	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle-<version>-1.x86_64.rpm	The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.
usp-auto-it-bundle-<version>-1.x86_64.rpm	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle-<version>-1.x86_64.rpm	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager-<version>-1.x86_64.rpm*	This package contains the script and relevant files needed to deploy the Ultra M Manager Service.

\* These bundles are also distributed separately from the ISO.

## 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](http://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](http://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)

© 2021 Cisco Systems, Inc. All rights reserved.