Release Notes for StarOS™ Software Version 21.23.6

First Published: July 29, 2021
Last Updated: July 30, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.23.5. 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	21.23.6, build 81507

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.

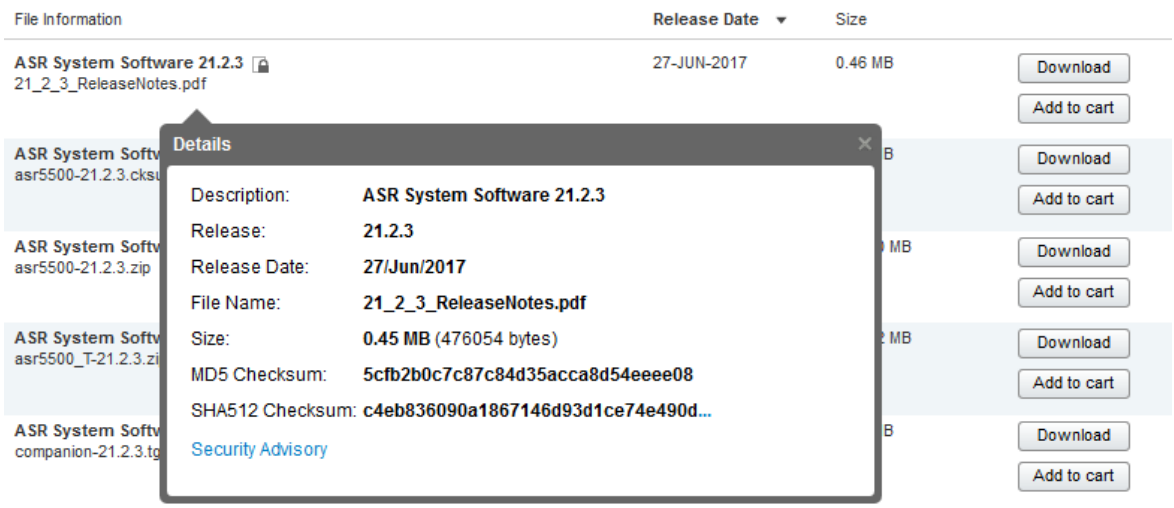
Firmware Updates

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

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 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*
CSCvz10703	[BP-CUPS]:session loss due to path-failure disconnection-reason	cups-cp
CSCvx28193	[BP-CUPS]:Assertion failure at sn_memblock_memcache_alloc() on UP ICSR	cups-up
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCvx87112	[BP-CUPS]: Fatal Signal 6 at smgr_match_pdr;uplane_match_pdr;uplane_execute_service_chain	cups-up
CSCvs05924	[URR] [SXAB] Updated URR doesn't exist	cups-up
CSCvx87105	[CP-CUPS]: Fatal Signal 6 at libc.so.6/__memset_sse2_rep	cups-up
CSCvx32019	"[BP-CUPS] Mid call predef rule changes from rated to free for all components, not charged correctly."	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvw76775	Many sessmgr restarts seen on virtual PGW	pdn-gw
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros

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

Resolved Bugs in this Release

The following table lists the known bugs that are resolved in this specific software release.

NOTE: This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the Cisco Bug Search Tool.

Table 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvw40208	CUPS QER Offending IE	cups-cp
CSCvz12277	CP Crash at acsmgr_dcca_process_msccs()	cups-cp
CSCvz12338	[BP-CUPS] UP-GROUP-NAME and UP-NODE-ID o/p not displayed in subs saegw-only all	cups-cp
CSCvx78549	[BP-CUPS] Observed restart sessmgr_pgw_fill_pgw_trans_node_from_sx_sef_out_info in Longevity run	cups-cp
CSCvw53667	[KT][CUPS] CP not properly handling UP URR message re-transmissions	cups-cp
CSCvw95981	sessmgr process restart at sgw_pdn_util_deallocate_sx_trans	cups-cp
CSCvw89176	"Gy CCR-U messages not sent to the OCS, and call proceeds without Quota"	cups-cp
CSCvy63788	Loss of LI X1 connection after CP reboot	cups-cp
CSCvw49535	Sessmgr reload at sess/egtp/egtpc/egtpc_utils.c:727	cups-cp
CSCvw54986	[BP-CUPS]: DS request is responded with No resource available during DS DB collision for PURES call	cups-cp
CSCvw95545	[CUPS-SAEGWC] Random CCR-U Flooding on Gx	cups-cp
CSCvx45708	[CUPS] [PGWCDR] - causeForRecClosing set to “Normal Release” when Sx Path Failure occurs	cups-cp
CSCvr99285	[CUPS] Counter in 'show radius counters summary' is not increment.	cups-cp
CSCvw65523	[CUPS CP] - CP fails to allocate a Peer-ID to UP following the UP Reload	cups-cp
CSCvx23431	Less than 16 rules are not working without CLI : no policy-control update-default-bearer	cups-cp
CSCvv74525	Non fatal vpnmgr restart on standby CP - seen every 24 hours	cups-cp
CSCvw02743	[STC CUPS] 3G call fail and session manager restart	cups-cp
CSCvw69965	Framed-IPv6-Prefix not included in Accounting-Request	cups-cp
CSCvw94565	[BP-CUPS] Inconsistency behavior in handling Predefined Rule and Group-of-Ruledef at control plane	cups-cp
CSCvw99517	[CUPS] Unexpected combinations of CRBN value and PLMN value in CDRs	cups-cp
CSCvx38502	Sessmgr sys-dump and config sync failure to standby noticed during ~10K ruledef config lines push	cups-cp
CSCvw76214	SCTP error logs are continuously output when diameter peer down	cups-cp
CSCvx13647	CP rejects DLDR session report by PDR is not present	cups-cp
CSCvx59719	negative value in show ip pool	cups-cp
CSCvy95216	[CUPS Pure-S] CUPS SGW is not including SGW S1-U TEIDs during piggyback CSR+CBR	cups-cp
CSCvv64417	[BP-CUPS][fapi 223801 error] api_transport.c:3448] fastpath_stream_change_state()	cups-up

Bug ID	Headline	Product Found*
CSCvw97015	"Sessmgr installing wrong TEP version in VPP, hence packets are dropped"	cups-up
CSCvx44355	ECS config mismatch observed between Active / Standby PGWU	cups-up
CSCvx61691	[UPF-SVI] :sessmgr restart at sessmgr_uplane_free_p2p_session()	cups-up
CSCvw67841	Rx packet lost by Tx Queue stuck on VPP tap interface on CUPS UP	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCvo47185	[BP-CUPS]Tos marked downlink pkts are counted twice in show sub cli.	cups-up
CSCvw60297	CUPS SRP over IPSEC - UPIMS - Periodic SRP flaps - need for cli to set tcp mss	cups-up
CSCvw73684	[CUPS UP] - Traffic Dropped with cause “R7Gx Rule-Matching Failure”	cups-up
CSCvv79637	"[SNMP]SNMP mib compilation errors seen for starServiceChainName, starUPlaneTsMissConfig"	cups-up
CSCvw04208	show subscribers user-plane-only callid <id> qos-group statistics not giving correct o/p on v21.x.gx	cups-up
CSCvx73933	CUPS UP - Packets stuck in VPP queue during OOO condition if stream is in config/pre-active state	cups-up
CSCvx82214	[BP-CUPS]Series of memblock crashes	cups-up
CSCvw83244	Uplink packet drops after 4g->3G handover on CUPS UP with this error: ADF UL TEID/QFI key mismatch	cups-up
CSCvv38100	CUPS - no bandwidth-policy and new bandwidth-policy config re-apply config deleted	cups-up
CSCvw76424	[BP-CUPS]Unable to start 4th mon sub session.	cups-up
CSCvw77581	[BP-CUPS] ruledef priority change and sx config push results in peering loss and outage	cups-up
CSCvx41375	CUPS-UP - New flows are created for every packet when 'logging monitor msid' is configured for UE	cups-up
CSCvw43171	[CUPS] [PFD Management] - Inconsistent rulebase configuration between CP & UP	cups-up
CSCvw91145	Display error in syslog for source ip address violation by IPv4 and IPv6 subscriber	cups-up
CSCvs23558	[BP-CUPS] PC: [048dd1d7/X] smgr_uplane_handle_config_chrg_action()	cups-up
CSCvy62199	[sol test] SM restart with fun: uplane_populate_edr_field_http_header_len()	cups-up
CSCvx69801	ruledef not getting removed in UP when “no ruledef” is configured and pushed to UP	cups-up
CSCvx83812	Sessmgr restart on standby UP @smgr_uplane_handle_load_optbldb()	cups-up
CSCvy64522	Fatal Signal 11: 11 PC: [04e301a8/X] sessmgr_uplane_sfw_nat_processing()	cups-up
CSCvu14090	[BP-CUPS] sessmgr restart at add_chunk() function	cups-up
CSCvw60349	[CUPS] NBR information is missing for subscriber-ipv4-address on port-chunk-release output	cups-up
CSCvy30776	Wrong CDRs are generated by PGW on receiving Secondary RAT Usage Reports in CNR	pdn-gw

Bug ID	Headline	Product Found*
CSCvy13275	show lawful-intercept imei returns No matching LI session/trigger found with active data session	pdn-gw
CSCvz00817	BP-ICUPS: Continuous VPP restart resulted in segmentation fault and callmodel failing	pdn-gw
CSCvy12988	Wrong CDRs are generated by SGW on receiving Secondary RAT Usage Reports	sgw
CSCvv69023	Cisco StarOS IPv4 Denial of Service Vulnerability	staros
CSCvw51050	21.14: Port speed OID changes after port up/down	staros
CSCvx98820	[CUPS-TACACS-IPsec] TCP connection failure with second tacacs server during failover	staros
CSCvw74776	VPNMGR process restart during Session Redundancy Test in SVI Testbed	staros
CSCvw15307	Sessmgr restart sessmgr_uplane_match_rule_after_cf	upf
CSCvx60658	[SVI-UPF]:Continuous sessmgr restart at sess/egtp/egtpu/egtpu_session.c:808	upf
CSCvw06261	"[UPF]:sn-start-time is not correct in transaction complete EDR, when there are multiple transactions"	upf
CSCvx08867	[Combo-UPF]Statistics issue for combo upf call where ACL is applied.	upf
CSCvx62133	Invalid content filtering policy id assigned to UE and potential sessmgr crash	upf
CSCvx72191	[UPF-SVI]: sessmgr restart at sessmgr_uplane_process_sx_sess_modify_remove_pdr_list()	upf
CSCvx38146	[UPF]:Incosistent behaviour for Change in content-ID not updating TEP row	upf
CSCvx85848	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_create_lc_record()	upf
CSCvy18530	UPF : UL ICMP packet is buffered even when UL FAR Action is forward	upf
CSCvx98495	[UPF-SVI] : sessmgr restarted at uplane_p2p_update_stats()	upf
CSCvy08954	[UPF-SVI] :sessmgr restarted at sessmgr_uplane_set_teid_pdr_binding_info()	upf
CSCvx92756	[UPF-SVI]: Sessmgr restarted at uplane_drv_handle_events_from_smgr()	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
CSCvy52016	Sessmgr restart during manual switchover on rolling upgrade	upf
CSCvx14614	"[Combo-UPF]Per peer statistics are incorrect for combo calls, in multi smf topology."	upf
CSCvy16147	"[UPF]Incorrect tos being marked for combo UPF, when charging action has tos and sgw marks inner pkt."	upf
CSCvx52114	[UPF]:pending-traffic-treatment quota-exhausted drop is not working as expected	upf

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

Operator Notes

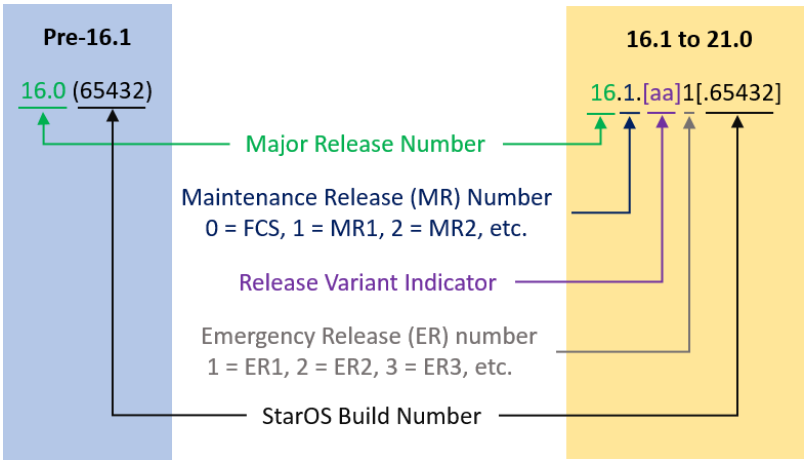
StarOS Version Numbering System

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

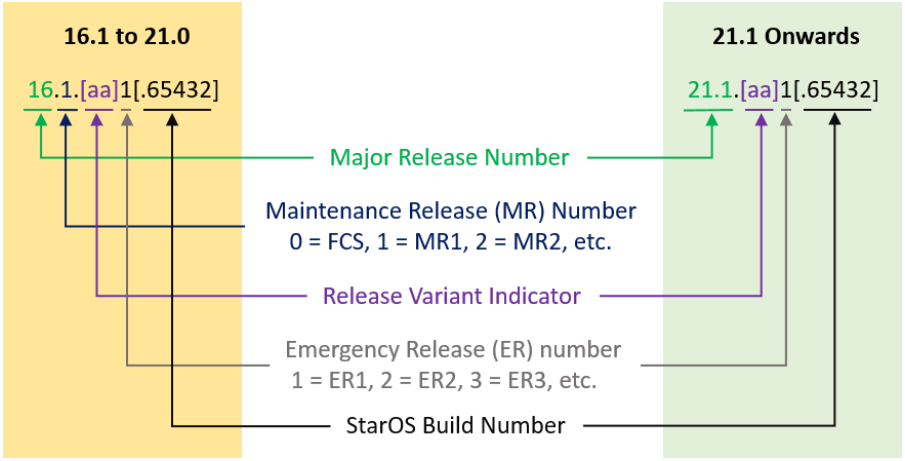
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build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

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

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



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



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

Release Package Descriptions

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

Table 5 - Release Package Information

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

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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-si-<release>.iso.zip	qvpc-si-<release>.iso	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
VPC Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 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 Table 6 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.