Release Notes for StarOS™ Software Version 21.22.n4

First Published: May 27, 2021
Last Updated: May 27, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.n3. 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	21.22.n4, build 80650

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.

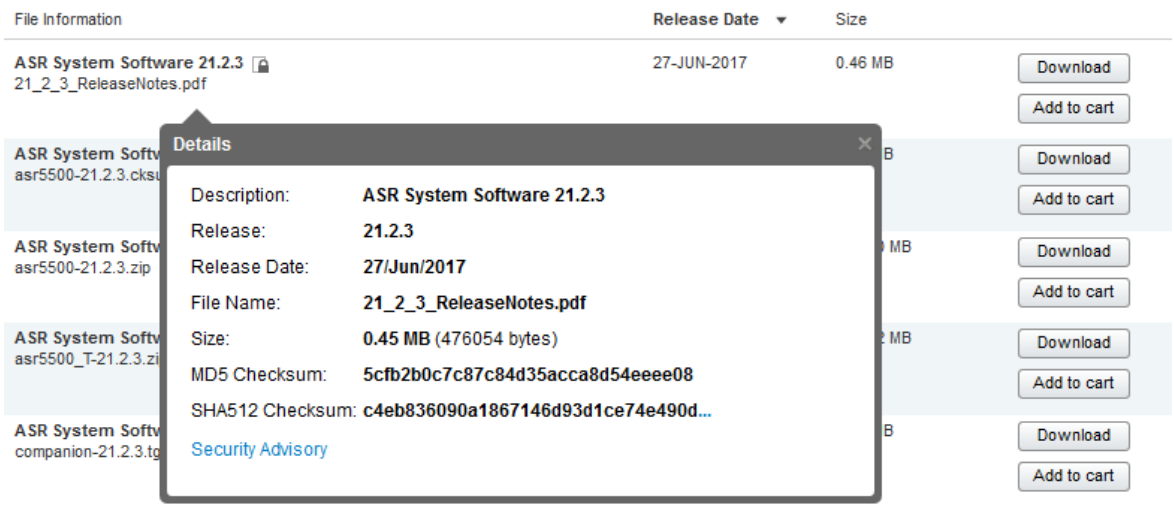
Firmware Updates

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 > 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*
CSCvw83826	[BP-CUPS]: Huge session disconnect with reason “sxfail-opr-remove-pdr”	cups-cp
CSCvx33850	Rulename associated with PDR is not displayed in “show cli” output	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
CSCvw58960	Sessmgr restarts at egtpu_process_tx_setup_req_evt()	cups-up
CSCvw04399	[BP-CUPS]SM restart after UP at ISCR sessmgr_Uplane_Uchkpt_clp_pdr_info.part	cups-up
CSCvx97927	[CUPS UP] - UP stuck in "UAANEPU" state after CP Reload	cups-up
CSCvx53094	sessmgr restart seen in function mme_app_fill_s1_bearer_values()	mme
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
CSCvs65524	[BP-ICUPS] HSUE UDP data not getting offloaded to VPP post RAR with MBR change	pdn-gw
CSCvv68655	[Legacy-GW] sessmgr sn_msg_chunk_rz_allocator_alloc_block()	pdn-gw
CSCvv89024	SM restart seen during LTE to eHRPD Handover.	pdn-gw
CSCvw25217	BP-ICUPS : sessctrl crashes during boot up at acs_sanitize_a_single_tdb	pdn-gw
CSCvw58020	Non WPS session : PGW not responding to MBReq - SRVCC without PS handover	sae-gw
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	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*
CSCvy33190	No CCR-U from CP after reception of Sx_Session_Report_Request with usage volume for VoGx	cups-cp
CSCvx00246	[CUPS / Sx] Unexpected Offending IE: UPDATE_PDR when switching rulebase	cups-cp
CSCvv74525	Non fatal vpnmgr restart on standby CP - seen every 24 hours	cups-cp
CSCvw40208	CUPS QER Offending IE	cups-cp
CSCvw70626	UE is not on CP but on UP causing DLDR session report rejection from CP	cups-cp
CSCvw89176	"Gy CCR-U messages not sent to the OCS, and call proceeds without Quota"	cups-cp
CSCvw95981	sessmgr process restart at sgw_pdn_util_deallocate_sx_trans	cups-cp
CSCvx13647	CP rejects DLDR session report by PDR is not present	cups-cp
CSCvx45708	[CUPS] [PGWCDR] - causeForRecClosing set to “Normal Release” when Sx Path Failure occurs	cups-cp
CSCvx59056	"CUPS-CP - After quota validity timer expiry, CP doesn't invoke Gy, leading to cc drops on UP"	cups-cp
CSCvx59968	CP sends wrong APN-AMBR (MBR) in QER in PFCP session modification request messages	cups-cp
CSCvx69017	Assertion failure at sess/smgr/sessmgr_saegw.c:8912 @ Function: sessmgr_delete_pending_timeout()	cups-cp
CSCvx72095	[BP-CUPS]: SessMgr restart @ sessmgr_snx_send_drop_call()	cups-cp
CSCvw99517	[CUPS] Unexpected combinations of CRBN value and PLMN value in CDRs	cups-cp
CSCvx08962	[CUPS SX] - Unexpected “LINKED URR ID” value (0x00000000) after Rulebase Change	cups-cp
CSCvx56945	[BP-CUPS] CDR not getting generated upon context replacement	cups-cp
CSCvw65523	[CUPS CP] - CP fails to allocate a Peer-ID to UP following the UP Reload	cups-cp
CSCvw95545	[CUPS-SAEGWC] Random CCR-U Flooding on Gx	cups-cp
CSCvw53667	[KT][CUPS] CP not properly handling UP URR message re-transmissions	cups-cp
CSCvw97371	[BP-CUPS]sn_slist_insert()smgr_uplane_handle_config_action_priority()sn_msg_arriving_handle()	cups-up
CSCvw97725	CUPS sessmgr restart on UPFdata - smgr_uplane_config_qos_gor	cups-up
CSCvx22765	CUPS UP sessmgr restart at acsmgr_process_get_grp_of_rdefs_stats	cups-up

Bug ID	Headline	Product Found*
CSCvx81075	[CUPS-UP] [MONSUB] wrong packet direction printed on console with User L3 PDU Decodes	cups-up
CSCvx98318	STC CUPS | Sessmgr restart while changing config of Gx-alias GOR	cups-up
CSCvx69801	ruledef not getting removed in UP when “no ruledef” is configured and pushed to UP	cups-up
CSCvx77929	'show ppp summary' restarts all sessmgr instances on CUPS-UP with active calls	cups-up
CSCvx86410	[STC CUPS] Rules are not hitting after modification in GOR	cups-up
CSCvx80819	[CUPS-UP] Stale session on UP after 3G session activation failure	cups-up
CSCvx82099	sessmgr restart seen in function sn_memblock_cache_get_mcblock_by_addr	cups-up
CSCvw54270	CUPS sessmgr restart on UPFData sessmgr_connproxy_client_state_cb	cups-up
CSCvx35980	[BP-CUPS] SR on UP after RAR with add+remove of gx-alias GoR causes data mismatch	cups-up
CSCvx60660	Task restart @ libc.so.6/__strlen_sse2_bsf()	cups-up
CSCvx73933	CUPS UP - Packets stuck in VPP queue during OOO condition if stream is in config/pre-active state	cups-up
CSCvw60297	CUPS SRP over IPSEC - UPIMS - Periodic SRP flaps - need for cli to set tcp mss	cups-up
CSCvx87599	MonSubProcessConnectFailure Error Message observed in Syslogs and SNMP trap	pdn-gw
CSCvw77989	Sessmgr restart while processing Secondary RAT Usage CDR records #2	pdn-gw
CSCvw58221	[BP_PCT PGW] Diameter data fragmentation not working as expected	pdn-gw
CSCvw47620	sessmgr restart seen after upgrade to 21.17.14 on acs_remove_learnt_cname_n_ip_addresses	pdn-gw
CSCvw67714	sessmgr restart when trying to fill in EDR with ULI encoded in hex format	pdn-gw
CSCvw95731	BP-ICUPS SegFault acsmgr_li_propogate_x3_table_idx_to_npu_response()	pdn-gw
CSCvx09943	[PLT-ICUPS]: VPP Crash Observed on Non Demux PDC2 card	pdn-gw
CSCvx28359	[BS-ICUPS] I-951 feature stats are not available after chassis reload & requires reconfig	pdn-gw
CSCvu87645	Wrong value of RX counter on 'show port utilization table'	sae-gw
CSCvw93927	All SESSMGR Crashes on hard reboot of compute VPC-DI	sae-gw
CSCvx16666	Sessmgr restart - Fatal Signal 6: Aborted PC: [093b7084/X] acsmgr_adc_dispatch_event()	sae-gw
CSCvx16689	sessmgr restart due to Segmentation fault PC: [0936e24b/X] acsmgr_tcp_optm_handling_uplink()	sae-gw
CSCvx62561	Observer High CPU on multiple cards with HO since 21.18.5 upgrade	sgw
CSCvx08467	Stale path keep remained after BGP shut	staros
CSCvw04670	DPC2 card failure due to IPS_ParityErrInt takes long to recover on ASR5500 node	staros
CSCvx08448	BFD remained as AdmDown after port no shut	staros

Bug ID	Headline	Product Found*
CSCvx16519	"VPC-SI |21.20.9| When querying virtual interface counters of the UP nodes, we see them all zeroed "	staros
CSCvx60658	[SVI-UPF]:Continuous sessmgr restart at sess/egtp/egtpu/egtpu_session.c:808	upf
CSCvw94672	VPP restart leading to reload of node and ICSR switchover	upf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

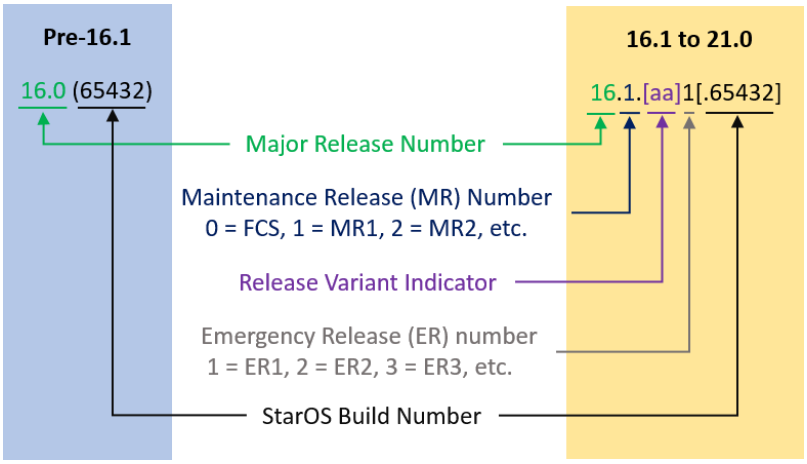
StarOS Version Numbering System

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.

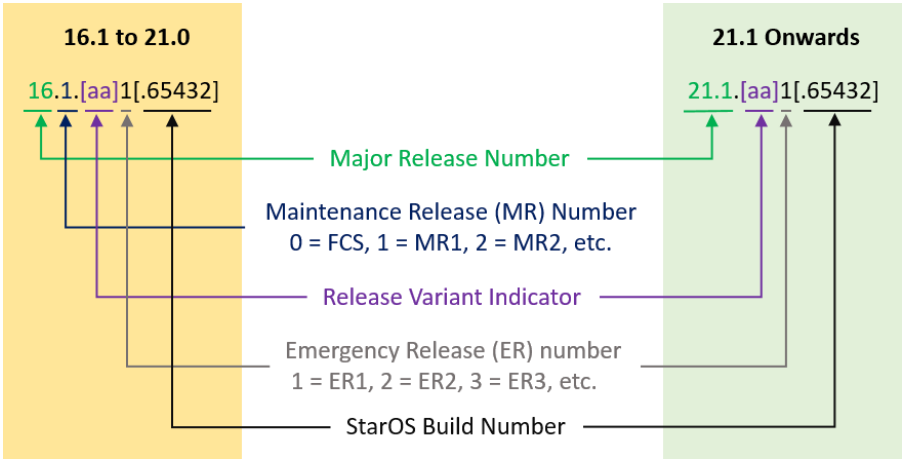
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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