Release Notes for StarOS™ Software Version 21.22.3

First Published: February 26, 2021
Last Updated: February 26, 2021

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.0. 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	21.22.3, build 79482

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.

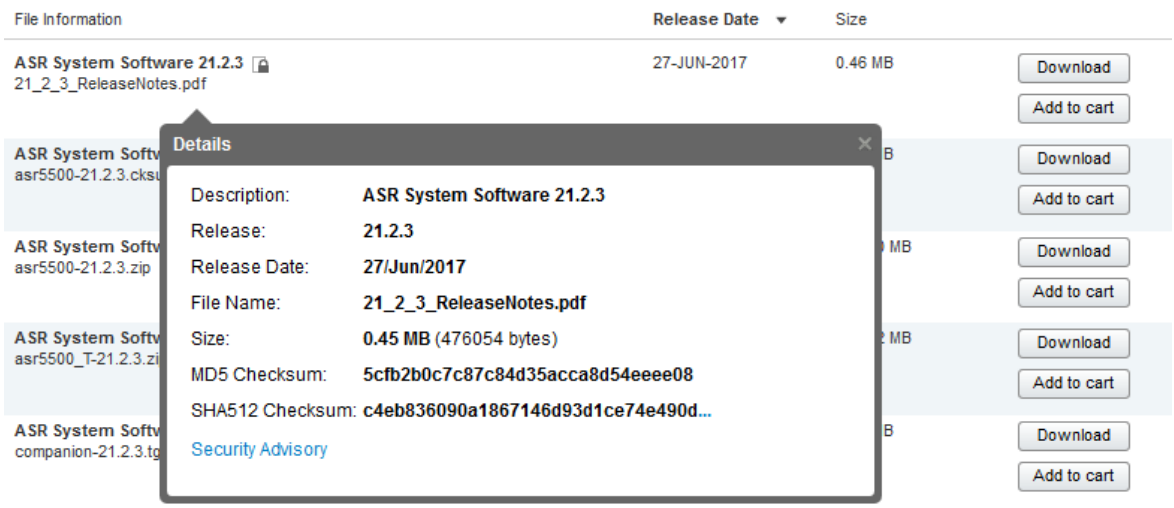
Firmware Updates

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*
CSCvx23431	Less than 16 rules are not working without CLI : no policy-control update-default-bearer	cups-cp
CSCvx33850	Rulename associated with PDR is not displayed in show cli output	cups-cp
CSCvx35944	[BP-CUPS] Rule mismatch in specific LTE-WiFi HO	cups-cp
CSCvx23410	[BP-CUPS] Removal of ruledef in gx-alias GoR using RAR is not updating the existing sessions	cups-cp
CSCvx40996	[SVI_UPF] Continuous restarts at PC: [f66d8fdd/X] libc.so.6/malloc_usable_size()	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
CSCvw89247	[BP-CUPS] Dynamic rule is not getting installed with no policy-control update-default-bearer	cups-up
CSCvw04399	[BP-CUPS]SM restart after UP at ISCR sessmgr_Uplane_Uchkpt_clp_pdr_info.part	cups-up
CSCvu37233	On VPC-DI Multiple Sessmgr restarts seen while doing SF card migration from active to standby	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
CSCvw51536	[I-CUPS] PC: [09e96246/X] acs_assign_data_session()	pdn-gw
CSCvw82177	BP-ICUPS : Sessmgr restarts when clearing full callmodel on the chassis	pdn-gw
CSCvx44104	[BP-ICUPS] I-951 - rules are not applied properly in the below callflow with buffering enhancements	pdn-gw
CSCvx38834	[BS-ICUPS] Buffered pkts stuck in the same state after EGTP_UPDATE_BEARER_REQ retransmissions stoped	pdn-gw
CSCvv89024	SM restart seen during LTE to eHRPD Handover.	pdn-gw

Bug ID	Headline	Product Found*
CSCvw58020	Non WPS session : PGW not responding to MBReq - SRVCC without PS handover	sae-gw
CSCvx03805	UPF: continuous ip address range pool of same network on multiple SMF is not working	upf
CSCvx14614	"[Combo-UPF]Per peer statistics are incorrect for combo calls, in multi smf topology."	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
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*
CSCvw89176	"Gy CCR-U messages not sent to the OCS, and call proceeds without Quota"	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
CSCvw95545	[CUPS-SAEGWC] Random CCR-U Flooding on Gx	cups-cp
CSCvw65523	[CUPS CP] - CP fails to allocate a Peer-ID to UP following the UP Reload	cups-cp
CSCvw02743	[STC CUPS] 3G call fail and session manager crash	cups-cp
CSCvw94565	[BP-CUPS] Inconsistency behavior in handling Predefined Rule and Group-of-Ruledef at control plane	cups-cp
CSCvw83244	Uplink packet drops after 4g->3G handover on CUPS UP with this error: ADF UL TEID/QFI key mismatch	cups-up
CSCvw60297	CUPS SRP over IPSEC - UPIMS - Periodic SRP flaps - need for cli to set tcp mss	cups-up
CSCvw97015	"Sessmgr installing wrong TEP version in VPP, hence packets are dropped"	cups-up
CSCvv79637	"[SNMP]SNMP mib compilation errors seen for starServiceChainName, starUPlaneTsMissConfig"	cups-up
CSCvw67696	[BP-CUPS]: Improper traffic matching to ruledef with ECSv2 enhancment feature enabled.	cups-up
CSCvw91145	Display error in syslog for source ip address violation by IPv4 and IPv6 subscriber	cups-up
CSCvx16840	"[CUPS] On a PGW-U switchover, IP pools are deleted from new Active UP, leading to traffic blackhole"	cups-up

Bug ID	Headline	Product Found*
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
CSCvu14090	[BP-CUPS] sessmgr restart at add_chunk() function	cups-up
CSCvw61491	[CP-MME] Sessmgr restarts seen at sn_list_contains_element	mme
CSCvw88936	[Cp-MME] MONTE: Error level log should be replaced with info level	mme
CSCvw84576	[21.15.48 FullVPP] PPTP-GRE Application protocol dropping Downlink packets towards UE	pdn-gw
CSCvw58221	[BP_PCT PGW] Diameter data fragmentation not working as expected	pdn-gw
CSCvw64306	PGW stops sending CCR/CCA when UBResp not received from previous PRA while new PRA is initiated.	pdn-gw
CSCvx08359	WiFi to VoLTE handover failure cause as CONTEXT_NOT_FOUND (0x40) with different pdn types	pdn-gw
CSCvw64863	[Smoke2-Legacy] TCP FIN/Reset are not sent post readdress rule install.	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
CSCvs09553	[BP-ICUPS]: Monsub pcap file's call id not changed after context replacement	pdn-gw
CSCvx08097	peer salvation feature not working as expected.	pdn-gw
CSCvu55467	[BP-ICUPS] Session Controller restart observed during data_backup_read_abort	pdn-gw
CSCvw95793	[Smoke2-ICUPS] In Monsub fastpath pcap files are not generated as expected.	pdn-gw
CSCvw67714	sessmgr restart when trying to fill in EDR with ULI encoded in hex format	pdn-gw
CSCvw73591	"ADC over Gx : Flow-description in CCR-U from PGW, sent ipv6 address with 0 prefix length."	pdn-gw
CSCvw95731	BP-ICUPS SegFault acsmgr_li_propogate_x3_table_idx_to_npu_response()	pdn-gw
CSCvw79616	sessmgr restart at sn_memblock_cache_get_mcblock_by_addr()	pdn-gw
CSCvw34433	[BP-ICUPS]Call cleared when CCRI towards OCS is sent mid-session	pdn-gw
CSCvx16689	sessmgr restart due to Segmentation fault PC: [0936e24b/X] acsmgr_tcp_optm_handling_uplink()	sae-gw
CSCvw64531	Revert from 21.22.x : ip user-datagram-tos copy command seems not effected in PGW	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
CSCvx08448	BFD remained as AdmDown after port no shut	staros
CSCvw04670	DPC2 card failure due to IPS_ParityErrInt takes long to recover on ASR5500 node	staros
CSCvw51050	21.14: Port speed OID changes after port up/down	staros
CSCvg20133	Segmentation fault at PC: [0d8e2647/X] EZprmSER_CheckError()	staros

Bug ID	Headline	Product Found*
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

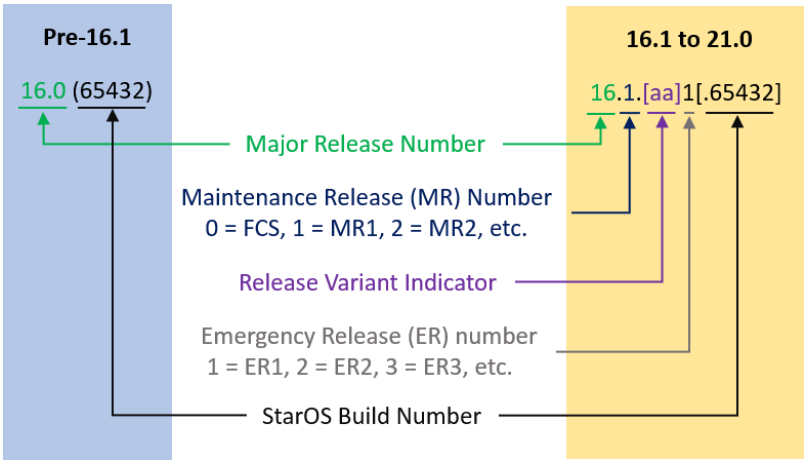
StarOS Version Numbering System

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.

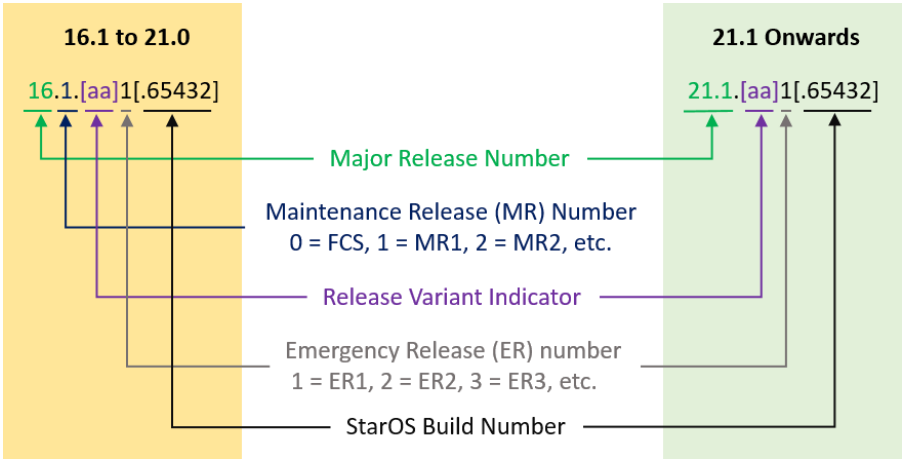
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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)