



Release Notes for StarOS™ Software Version 21.27.5

First Published: November 30, 2022

Last Updated: November 30, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.27.4. These release notes are applicable to the ASR5500, VPC-SI ,VPC-DI platforms and RCM platform.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.27.5, build 87852

Feature and Behavior Changes

For information on feature and behavior changes associated with this release, refer to the [CUPS Release Change Reference](#), and the corresponding [StarOS Release Change Reference](#).

Related Documentation

For the complete list of CUPS documentation available for this release, go to <https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html>.

For the complete list of the corresponding StarOS documentation, go to <https://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.

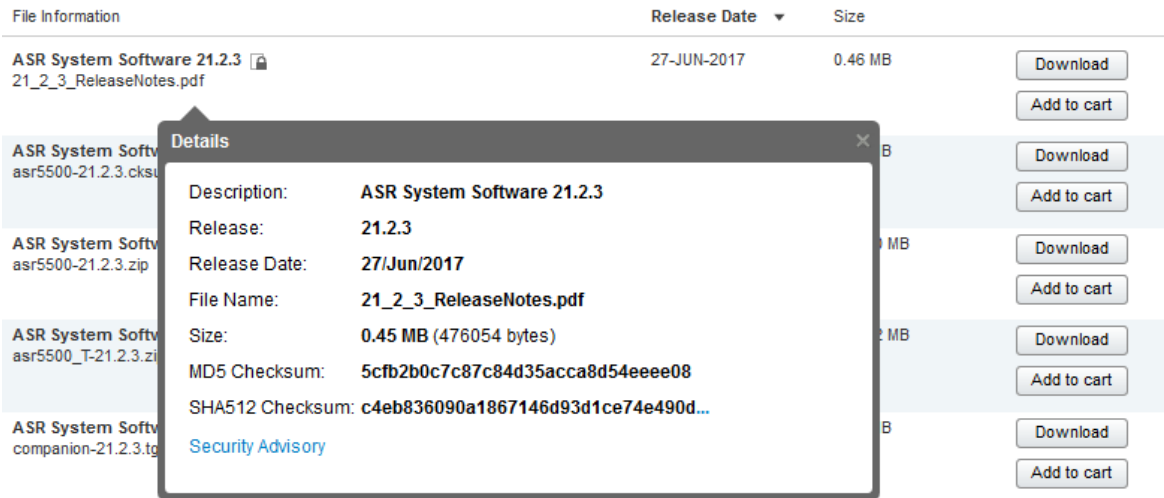
Firmware Updates

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

Open Bugs in this Release

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*
CSCwd67633	[BP-CUPS]libvnet.so.19.08.1/vlan_ip4_qos_mark_node_fn_avx2() with vpp restart	cups-up
CSCwc12852	[CUPS-BP] Admin Guide - Servers Unreachable - Specify non-support for after-timer-expiry	cups-cp
CSCwc81923	CUPS LI Admin guide needs to remove SaMOG and ePDG related support	cups-cp
CSCwd70319	[BP-CUPS]rmmgr crash PC: [f667acb3/X] libc.so.6/__memcpy_ia32()	cups-cp
CSCvz92617	[BP-CUPS]:Huge number of error logs observed acsmgr_populate_chrg_info_from_urr failure	cups-cp
CSCwd09301	RMMGR in Warn State on all Active SFs of CUPS-CP	cups-cp
CSCwa83375	[BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup	cups-cp
CSCwc34754	Active call got disconnected during handoff from 4G to wifi on ICSR setup with Gx-Alias enabled.	cups-cp
CSCwd39954	[CUPS-CP] Delay seen when CP handles 32 Sx associated UPs	cups-cp
CSCwd08502	[CUPS CP] MBR reduced to 1Kbps during 4G to 3G handoff if 4G AMBR is 4294968	cups-cp
CSCwd19379	[BP-CUPS] call drops on sessmgr task kill - recover_sgx_from_crr failed	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwc95490	Assertion failure at sess/sctrl/sessctrl_rcm.c:326-Func-sctrl_config_rcm_service()	cups-up

Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwd70361	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23427	cups-up
CSCvz03179	[BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases	cups-up
CSCwc82316	"Recovery after Gy bypass (SU for CCR-I/CCR-U), UP drops all subscriber packets"	cups-up
CSCwc97265	[BP-CUPS]Recovery after Gy bypass - CP does not send UPDATE PDR for predefined rules	cups-up
CSCwc97902	[BP-CUPS] V6 peers not coming up due to cause PFCP_CAUSE_REQUEST_REJECTED	cups-up
CSCwc53344	[BP-CUPS] Function: Assertion failure sessmgr_func.c:37116 Function: sessmgr_get_session_entry	cups-up
CSCwd19318	Enabling masked-imeisv only working for one mme-service when there are 2 mme-service	mme
CSCwc95163	"[NSO-MOB-FP] p2p plugin has since release 2.65, 4 sets of digits with one ER value"	nso-mob-fp
CSCwa79744	BP-ICUPS : CUSP Feature not working in 21.27.x builds	pdn-gw
CSCwb66185	Document: Removal of Step2 under the Generating SSH Client Key Pair	pdn-gw
CSCwa75121	UPF doesn't trigger Sx Session Report for Volume Threshold breach intermittently	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*
CSCwc50029	CUPS-CP sessmgr_sgw_handle_delete_req()	cups-cp
CSCwc97995	[CUPS CP]: WIFI to LTE handoff failure due to EBI mixing with dedicated bearer	cups-cp
CSCwc80718	CUPS CP: Memory leak in sn_memblock_cache_alloc_new due to acsmgr_wrap_far_cache	cups-cp
CSCwd29916	IP Pool-ID changes after reload - causing call recovery failures in CP ICSR setup	cups-cp
CSCwc88588	"CUPS-CP - After quota holding timer expiry, CP doesn't invoke Gy"	cups-cp
CSCwc98188	sessmgr crash on CUPS-CP when UE is trying for more than 11 bearers	cups-cp
CSCwc78237	"[BP-CUPS] [sessmgr 10699 error]Misc Error:3G UE < 0, error code 0,Misc Error: 2G UE > 0,error code 0"	cups-cp
CSCwd40148	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwc42889	CUPS: SGW CDR containing wrong (future) timestamp in "record opening time"	cups-cp
CSCwc84548	[CPUS-CP] [ICSR] SRP Standby CP sending Sx Session Delete Request which is not expected	cups-cp

Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwd39782	[BP-CUPS] root-dir line in the local context sshd configuration is missing after reboot of StarOS	cups-cp
CSCwc87052	Sessmgr gtpu restart at gtpu_sess_abort_handler	cups-cp
CSCwa98422	[BP-CUPS]observed smgr restart "acsmgr_check_n_delete_pdrs_for_deleting_bearer" in Longevity run	cups-cp
CSCwc66274	[CUPS-CP] "Requested-Service-Unit" AVP missing after receiving CCRI with 0 GSU and Redirection	cups-cp
CSCwc77597	High sessmgr utilization on CP due to memory leak from DNS NAPTR queries	cups-cp
CSCwc49447	CP not forwarding PCC dynamic rules to UP over Sx	cups-cp
CSCwd06686	[CUPS-CP] SessMgr restarts on Sec rat trigger hitting threshold with 2 def bearers for pure-S calls	cups-cp
CSCwc54584	[CUPS][npumgr-drv 185001 error vpp_tcp_conn_bind_cb_v6_v4: VPP-LI: Fail to add socket with dhost	cups-up
CSCwc53608	[(libvnet.so.19.08.1/ip4_rewrite_node_fn_avx2()) [(libvlib.so.19.08.1/dispatch_pending_node	cups-up
CSCwc44211	CUPS UP - Upgrade from 21.23.n9 to 21.23.n10 observed higher RTT/delay between S1U/SGi	cups-up
CSCwd33488	[CUPS UP] Large sx messages retransmission from CP if ipsec is used in Sx	cups-up
CSCwc87274	"CUPS,VPP restart in vlan_ip4_qos_mark_node_fn_avx2"	cups-up
CSCwc81666	[CUPS RCM] RCM trying to create the server list before the UP instance created	cups-up
CSCwc76586	IPv6 src IP corruption for UDP LI in CUPS	cups-up
CSCwd10414	OFR Requirement to enable DH Group 5 in 21.27	epdg
CSCwc67866	Invalid container time of last-usage values	pdn-gw
CSCwd41111	[S8HR] SGW increments "Apn Lookup Failed" wrongly for packets sent over non-s8hr bearers	pdn-gw
CSCwd02729	Continuous EGTPCPathFailClear traps after receiving echo requests during no session	pdn-gw
CSCwc09456	Sessmgr instance restart due to assertion failure at acs/acsmgr/acsmgr	pdn-gw
CSCwc80092	Flows are getting terminated even before the configured flow limit is reached	pdn-gw
CSCwc44793	Sessmgr task restart on acsmgr_config_acs_rule_options() during ECS config change	pdn-gw
CSCwd64943	[SAEGW]: ICSR Standby sessmgr in Memory over state	sae-gw
CSCwb55423	[VPC-DI] Sessmgr process restart at sessmgr_pgw_fill_event_record_csr	sae-gw
CSCwd17939	"In sGWRecord, changeTime appearing as before time from recordOpeningTime and duration showing zero"	sae-gw
CSCwd41016	No session deletion after S5 path failure followed by bearer resource command	sgw
CSCwc69565	[S8HR] show lawful-intercept s8hr statistics all display the wrong ebi value	sgw
CSCwc99662	SGW sessmgr task restart observed with bearerResourceCmd during S5 path failure	sgw
CSCwb75361	[S8HR] sessctrl restart sessctrl_handle_s8hr_apn_list	sgw

Operator Notes

Bug ID	Headline	Product Found*
CSCwd17474	Trusted build: StarOS password encryption improvement feature new format saving issue	staros
CSCwd49072	Improve detection of invalid qem entry access	staros

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

Operator Notes

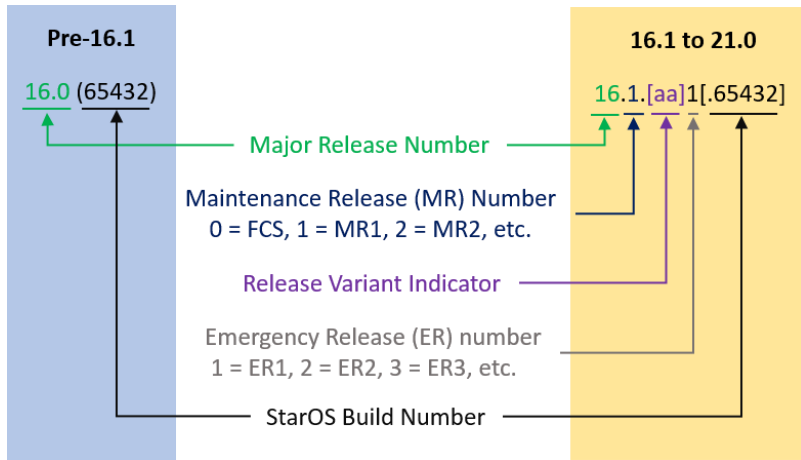
StarOS Version Numbering System

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.

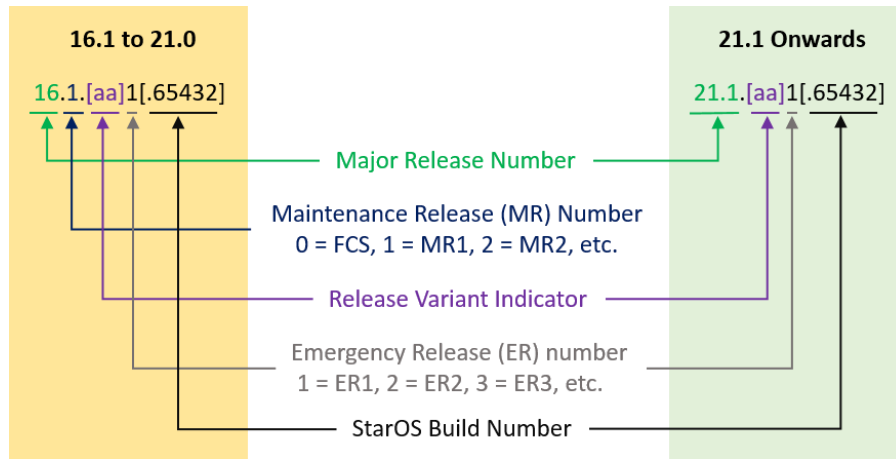
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

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".

Operator Notes



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	<p>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.</p> <p>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.</p>
VPC-DI		
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	<p>Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	<p>Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	<p>Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	<p>Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>

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

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

© 2022 Cisco Systems, Inc. All rights reserved.