



# Release Notes for StarOS™ Software Version 21.25.16

First Published: May 29, 2023

Last Updated: May 29, 2023

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.25.15. These release notes are applicable to the ASR5500, VPC-SI ,VPC-DI and RCM platforms.

## Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.25.16, build 90072

## Feature and Behavior Changes

Refer to the [Release Change Reference](#) for a complete list of feature and behavior changes associated with this software release.

## Related Documentation

For a complete list of documentation available for this release, go to <http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html>.

## Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

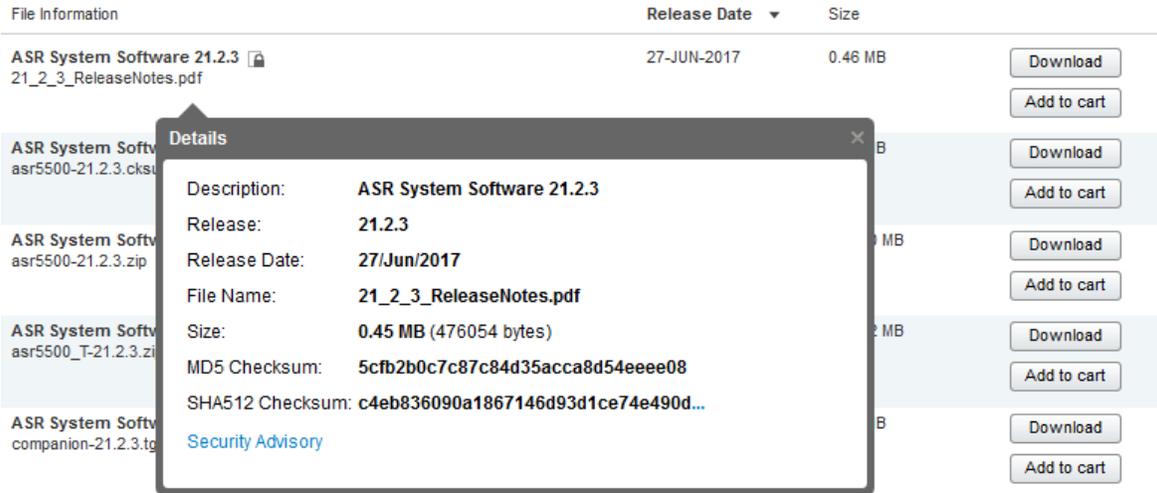
## Firmware Updates

There are no firmware upgrades required for this release.

## Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **Cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To validate the information, calculate a SHA512 checksum using the information in [Table 2](#) and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop see [Table 2](#).

**Table 2 - Checksum Calculations per Operating System**

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

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

## Certificate Validation

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

## Open Bugs in this Release

The following table lists the known bugs that were found in, and remain open in this software release.

**NOTE:** This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the [Cisco Bug Search Tool](#).

**Table 3 - Open Bugs in this Release**

Bug ID	Headline	Product Found*
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running call model	cups-cp
CSCwd40162	[BP-CUPS] sesmgr crash: Assertion failure at sess/smgr/sessmgr_fsm_func.c:10998	cups-cp
CSCwd55835	Pure-P to Collapsed and Collapsed to Pure-P Handovers are supported in CUPS	cups-cp
CSCwe30123	VPC - [SAEGW] - 21.25.10 (86143) - High level of service denied on SAEGW	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwd19632	Assertion failure at sessmgr_app_svr_event_control_dispatch	cups-cp
CSCwd60353	CUPS - SAEGW - 21.25.10 - acsmgr_process_qgr_and_create_pdr_far	cups-cp
CSCwe61003	[CUPS-CP] Unexpected "URR node not found at CP for URR-id" logs observed	cups-cp
CSCwa08379	APN without IP pool name not able to serve call despite having free IPs.	cups-cp
CSCwa54600	[BP-CUPS] Assertion failure @ PC: [08dc3801/X] fill_dyn_chrg_rule_name_info()	cups-cp
CSCwd14939	[CUPS-CP] Incorrect duration for time limit triggered CDRs after configuration change	cups-cp
CSCwd34520	CUPS (21.25.10) Assertion failure at sess/smgr/sessmgr_pgw.c:21482	cups-cp
CSCwd40067	4G QOS sent on UP after CCA-U while UE still in 3G	cups-cp
CSCwd10514	CUPS 'clear subscribers' documentation updates	cups-cp
CSCwc07644	[BP-CUPS]AF at sess/smgr/sessmgr_gr_sess.c:1368 sessmgr_gr_handle_session_full_checkpoint on standby	cups-cp
CSCwc21399	[BP-CUPS][sx 221332error<sessmgr:23>sx_db.c:1238]Tunnel_record local seid and Packet seid does not	cups-cp
CSCwe71916	Sessmgr restart due to assertion failure in pgw_drv_fill_bearer_info_from_egtpc function.	cups-cp
CSCwc42330	Observed Sessmgr crash on CP:: "sessmgr_pgw_handle_create_bearer_cfm"	cups-cp

## Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwe91366	"URR node not found at CP for URR-id" of URR-id ended with 1 or 2	cups-cp
CSCvz73626	sessmgr assert @ smgr_uplane_config_rule_options()	cups-up
CSCwa92931	[CUPS-LI-TLS] X3 index for heartbeat is not removed after removing LI config	cups-up
CSCwf27682	Sessmgr's memory is contiously increasing in KT corporation	cups-up
CSCwb55459	[BP-CUPS]:Assertion failure at sctrl_cfg_sync_decode_traffic_optimization_profile_config_tlv()	cups-up
CSCwf03759	CUPS UP sessmgr core file generated on SRP Standby node	cups-up
CSCvz49026	[BP-CUPS] sessmgr restart @ sn_memblock_memcache_alloc()	cups-up
CSCwb16852	"F102857 : ECS config corrupted on UP, after removing Sx-Association or removing ECS config on CP"	cups-up
CSCwb75761	Multiple session manager restart - sessmgr_process_init_config	cups-up
CSCwd91434	[CUPS-UP]: Assertion failure at 'smgr_uplane_opt_hash_table_deinit on UP	cups-up
CSCwe62837	difference between CUPS and ASR5500 in case of redirected flow getting reclassified	cups-up
CSCwf12887	Fatal Signal 11: smgr_uplane_rule_compare_icmp_type()	cups-up
CSCwe70286	"ePDG PLMN handoff attempts,success counters having same values in CLI"	epdg
CSCwd68562	ASR5500 - MME- 21.25.4 (83215) - MMES1PathFail increase	mme
CSCwd38978	MME is not responding to default IMS PDN Connectivity message	mme
CSCwe51260	mmemgr crash	mme
CSCwf01774	Sessmgr Crash @Assertion failure at sess/mme/mme-app/app/mme_app_util.c:22169	mme
CSCwb69510	The assert is hitting when mme handles the context response with failure cause code from the peer	mme
CSCwb59168	Encoding error @Stop-Warning-Indication message for multiple eNB-ID in "Broadcast-Empty-Area-List"	mme
CSCwc60621	MME: Assertion failure at sess/mme/mme-app/app/mme_app_egtpc.c:10901	mme
CSCwd17450	DDN option available under network-overload-protection cli not showing TEID-0 info	mme
CSCwc93508	MME Sending incorrect TAC to SGW on Delete Session Request messages	mme
CSCwc95044	MME continues to use blockedlisted SGW	mme
CSCwf10919	Debug code to troubleshoot SessMgr restart while handling Modify Bearer request	mme
CSCwd52626	Assert at egtpc_resume_suspended_proc()	mme
CSCwd38108	Documentation: cli after-attach information not included in user guide	mme
CSCwd71339	Increase in DUCON_NSA errors / path switch failures	mme
CSCvz46024	[CP-MME] sessmgr restart at egtpc_handle_mod_bearer_cmd_req_evt	mme

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwc82786	MME Sending twice ULR as part of 5g-4g HO Followed by TAU	mme
CSCwd40838	mme sessmgr restart at mme_app_do_sgw_dns_query	mme
CSCwd91474	New calls are accepted even new call policy is configured as reject	mme
CSCwe21358	"KPI Counters / Bulk Stats for Extended QCI (65, 69) not available"	mme
CSCvy90872	"BP-ICUPS: VPP restart while running the callmodel, resulted in segmentation fault"	pdn-gw
CSCwa54994	BP-ICUPS: sm reload at sn_memblock_cache_block_flush.part.1()	pdn-gw
CSCwc97269	APN configuration getting removed	pdn-gw
CSCwd12198	[ICUPS-Smoke2] Assertion Failure @ acsmgr_config_acs_rule_options	pdn-gw
CSCvz76252	[BP-ICUPS] buffer leak found at VPP with regular callmodel sessions on the chassis	pdn-gw
CSCwa41502	BP-ICUPS: sessmgr segmenattaion fault at sn_msg_arriving_handle()	pdn-gw
CSCwa11844	BP-ICUPS: aaamgrs are going to over state due to high memory usage	pdn-gw
CSCwa50873	Many session disconnect reasons are not documented	pdn-gw
CSCvz70919	RCM OVF deployment for 21.25.x image is not succeeding	rcm
CSCwc26449	[PLT-RCM] Ubuntu 18.04 LTS / 20.04 LTS / 21.10 / 22.04 LTS : OpenSSL vulnerability (USN-5488-1)	rcm
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCvz61597	[SGIR-Ph1] After first switchover some profiles are in unknown state initially in save & reload case	sae-gw
CSCvz65453	[SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN	sae-gw
CSCwb65556	Observing sessmgr crash:: sessmgr_get_num_mnc_digits	samog
CSCvz94977	Maximum number of NTP servers	staros
CSCvy50485	[SVI-UPF]: vpp restarts at sn_assert_signal_handler()	upf
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	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*
CSCwf11062	Sessmgr restart after GTP-C path failure	cups-cp

Operator Notes

Bug ID	Headline	Product Found*
CSCwc53608	[[libvnet.so.19.08.1/ip4_rewrite_node_fn_avx2()]] [[libvlib.so.19.08.1/dispatch_pending_node]]	cups-up
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

## Operator Notes

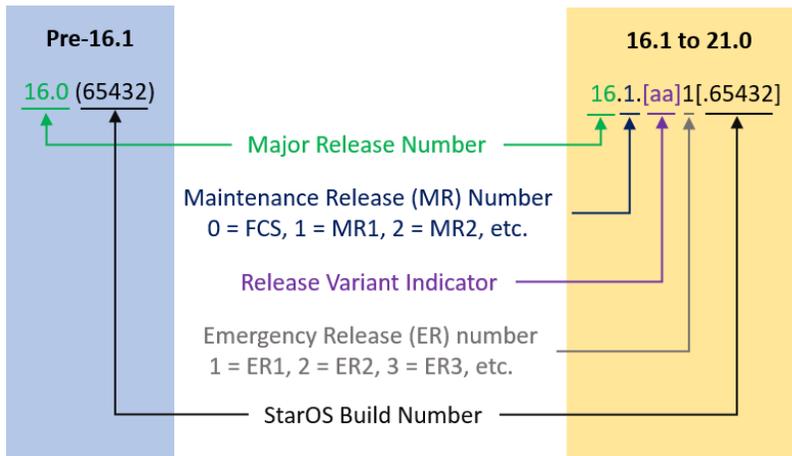
### StarOS Version Numbering System

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

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

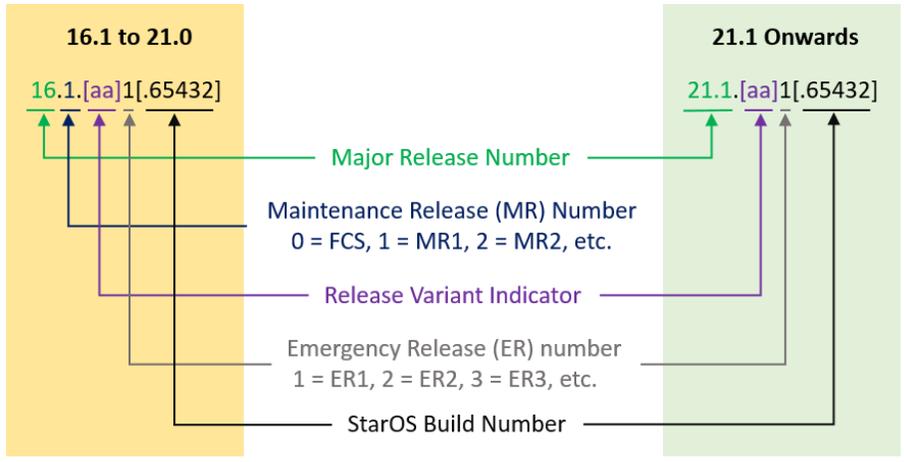
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

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



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

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

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

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>

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

**Table 6 - USP ISO Bundles**

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

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.