Release Notes for StarOS™ Software Version 21.23.n9

First Published: March 31, 2022
Last Updated: March 31, 2022

Introduction

This Release Note identifies changes and issues related to this software release. These Release Notes identify changes and issues based on 21.23.n8

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.23.n9, build 84522

Descriptions for the various packages provided with this release are located in Release Package Descriptions.

Feature and Behavior Changes

Please contact the Account team for the documentation related to 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 installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

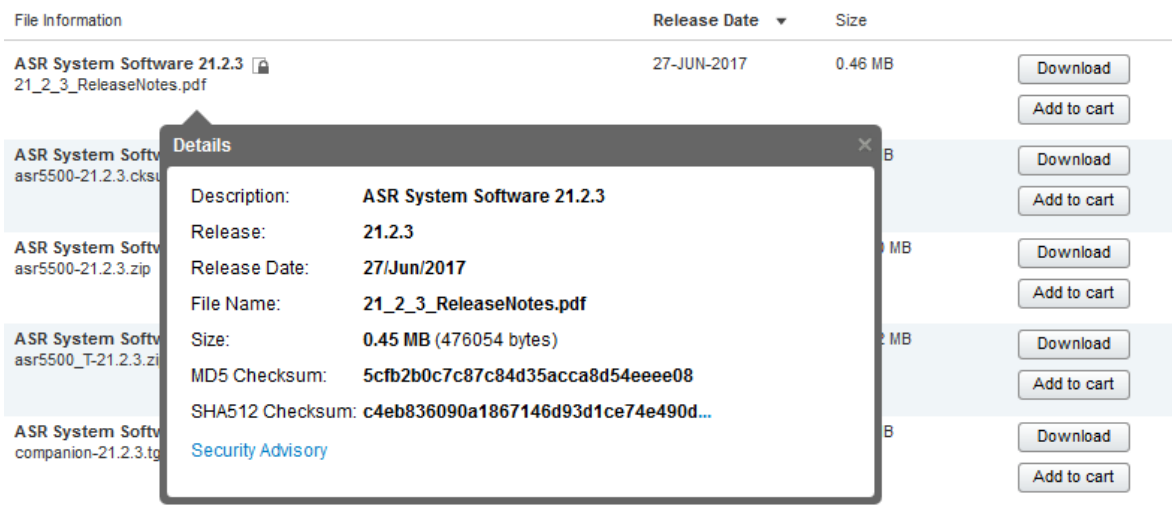
There are no firmware upgrades required for this release.

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 the following mechanisms:

- **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.

- **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

  <product>-<version>.cksums

  Example: asr5500-21.4.0.cksums

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 please see the table below.

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>*

Operating System	SHA512 checksum calculation command examples

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/or that 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*
CSCwa75035	CoCUPS: UP-IMS performance below commitment	cups-up
CSCwb06340	[CUPS] SGW does not always properly handle release access bearer with 2 sessions	cups-cp
CSCwb16706	[CUPS] sn_assert() egtpc_handle_rel_access_bearers_rsp_evt() egtpc_handle_user_sap_event()	cups-cp
CSCwa87274	[UPF] Sessmgr crash : uplane_sfw_nat64_translate_ipv6_to_ipv4 during call running model	cups-up
CSCvz66300	[BP-CUPS]: Huge number of session disconnection observed related to sx	cups-cp
CSCwa41564	[BP-CUPS] Current “NAT IP” not cleared post call clear and NBR expiry	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp

Bug ID	Headline	Product Found*
CSCvz92617	[BP-CUPS]:Huge number of error logs observed acsmgr_populate_chrg_info_from_urr failure	cups-cp
CSCwa52727	[BP-CUPS] Sessmgr crash @sx_handle_user_sap_event() when removing the LI configs	cups-cp
CSCvz90294	smgr_uplane_handle_config_timedef() restart is seen on ICSR UP	cups-up
CSCvz51704	[BP-CUPS]: Segmentation fault at VPP	cups-up
CSCwa92902	[BP-CUPS] Assertion failure at PC: [f67cb491/X] libc.so.6/__memcmp_sse4_2()	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCwa33605	[CUPS] Error logs DNS snooping: unexpectedly p_hentry is NULL observed (even after fix in 21.23.11)	cups-up
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCwa36635	MME crashes after upgrade to v21.23.6_21_mme_fsm_event_handler()	mme
CSCwa83203	Observing sessmgr restart::sessmgr_egtpu_receive_gtpu_v6_packet	pdn-gw
CSCwa23914	sessmgr restart due Fatal Sig PC: [09fd165b/X] acsmgr_sess_sr_uchkpt_delete_all_accnt_mscc_bucket()	sae-gw
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvz16012	GMPC event not triggering with reporting action for 3g Detach	sgsn
CSCvy31013	DNS queries not leaving the chassis in certain situations	staros
CSCvz28910	Supporting 25G link speed in staros linux kernel code for drivers(i40evf)	staros
CSCwa40585	Vpnmgr restart @ vpnmgr_check_addr_conflict()	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Resolved Bugs in this Release

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

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

Table 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwa79275	CUPS CP Sending GoR name in absence of Ruledef in Rulebase and no Ruledef installed for subscriber.	cups-up
CSCwa98433	"CUPS-UP: if CP reloads after unsuccessful config push, standalone UP does not re-establish sx assoc."	cups-up
CSCwa49671	sessmgr restart at sess/imsa/src/imsa_srvr.c	cups-cp
CSCwb06211	CUPS CP :counter SAEGW.pgw-sesstat-pdn-rat-geran is never reset on 21.23	cups-cp
CSCwb08731	[CUPS] CP does not request quota following "start-of-traffic" report from UP	cups-cp

Bug ID	Headline	Product Found*
CSCwa33658	sessmgr 12325 error “Uplane received invalid far id in PDU”	cups-cp
CSCwa40159	[CUPS] Assertion failure Function: sessmgr_ggsn_handle_pcc_intf_evt_policy_change_ind	cups-cp
CSCwb00982	Observing sessmgr crash::sgwdrv_get_bearer_info_data	cups-cp
CSCwb02662	[CUPS CP] sessmgr restart is seen in Function: sn_aaa_session_set_user_data()	cups-cp
CSCwb03324	CUPS CP - Unexpected UPC request from CUPS GGSN after QOS change in 3G occurs	cups-cp
CSCwa78352	"[CUPS] SMGR_GGSN_SX_MODIFY_REQ_LI or SMGR_PGW_SGW_MODIFY_REQ_LI req to send Mod Req failed for LI,"	cups-cp
CSCwa90459	[BP-CUPS]:Sessmgr restarts at sn_memblock_memcache_free() leads to call drops	cups-cp
CSCvz19221	UP response PFCP_CAUSE_REQUEST_REJECTED in SX_SESSION_MODIFICATION processing	cups-cp
CSCwa61799	[CUPS] 4G->2G/3G->4G HO failures - double traffic endpoint deletion	cups-cp
CSCwa78138	[CUPS] CUPSSefCache free does not come back to 200 - Loss	cups-cp
CSCwa80683	[CUPS] Fatal Signal 11 - sn_memblock_cache_free_new / acsmgr_free_cups_sef_info	cups-cp
CSCvz64321	[BP-CUPS] Observed error sgwdrv_fill_sess_info_from_egtpc_temp_pdn_ingress in Longevity setup	cups-cp
CSCwb07764	CUPS UP: nat-binding-timer is not respected strictly	cups-up
CSCwa83817	[CUPS-UP] Some UP does not activate VPP correctly after upgrade or reload	cups-up
CSCwb08945	[BP-CUPS] Sessmgr crash @sessmgr_uplane_process_sx_remove_far () during the LTE to Wifi HO.	cups-up
CSCvz28964	Fatal Signal 6: 6 PC: [ffffe430/X] __kernel_vsyscall()	cups-up
CSCwa42645	EDR attribute rule-variable charging-id not capturing values or missing values in EDRs for pure-p	cups-up
CSCwa77273	wrong detection for whatsapp traffic	cups-up
CSCwa38971	[CUPS] PSF - Config “firewall icmp-fsm” block some ICMP responses expected (sollicited)	cups-up
CSCwa41897	[CUPS] APN bulkstat data-touseravg-pps and data-fromuseravg-bps are counting SGW traffic	cups-up
CSCwa67585	[CUPS UP] UP is creating using each NAT port for every ICMP and never release [Stuck NAT Chunks]	cups-up
CSCwa68337	[BP-CUPS] Crash at sessmgr_clear_teid_pdr_binding_info_list() on performing HO	cups-up
CSCvx13009	"In CUPS nodes IMS subs facing one way audio , intermittently"	cups-up
CSCwa39049	UBR Buffering is partially working	mme
CSCwa83584	Assertion failure at sess/mme/mme-app/app/mme_egtp_fw.c:1078	mme
CSCvx66314	sessmgr restart during recovery due to local teid mismatch	mme
CSCvy05245	Session manager crash at sess/egtp/egtpc/egtpc_utils on MME	mme
CSCvy13440	Session manager restart observed after embms session start procedure from MBMS GW.	mme
CSCvy33330	Need IPv6 pgw-address support under apn profile without EPDG/SMOG license components	mme
CSCvy88049	[MME] Flood of mme-app unusual “Invalid bearer Id..!” logs	mme

Bug ID	Headline	Product Found*
CSCvz69392	%emm-msgtx-emergency-disabled% stats incrementing wrongly	mme
CSCvz96103	Unexpected EMERGENCY_CALL_ORIGINATION messages from the MME to the GMLC	mme
CSCvz60305	PLT-ICUPS-21.25: VPP_main facility is going to OVER state while Call model test is in progress	pdn-gw
CSCwb06206	CUPS CP: Syslog with Misc error: Updating Micro Checkpoint. number of bearers	sae-gw
CSCwa94328	[BP -CUPS] Sx down after SF reboot followed by CF switchover	staros
CSCwa65688	[UPF] Sessmgr crash- uplane_populate_edr_field_bearer_charging_id while generating session-end edr	upf
CSCwa92472	Packet drop at sessmgr after atomic frag header removal	upf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

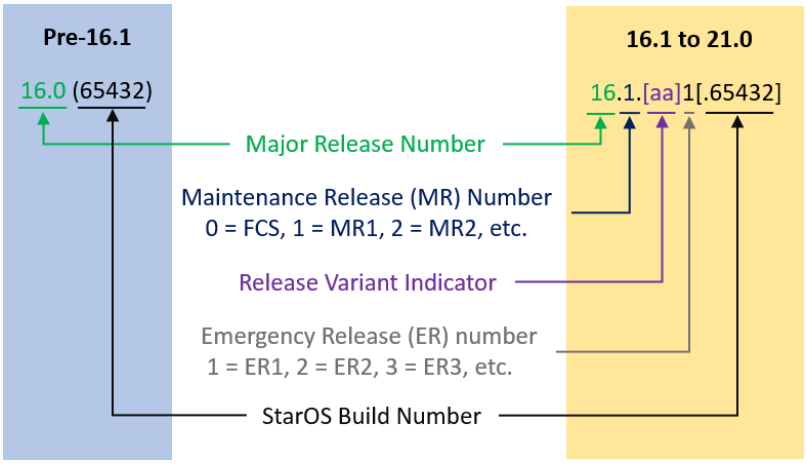
StarOS Version Numbering System

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

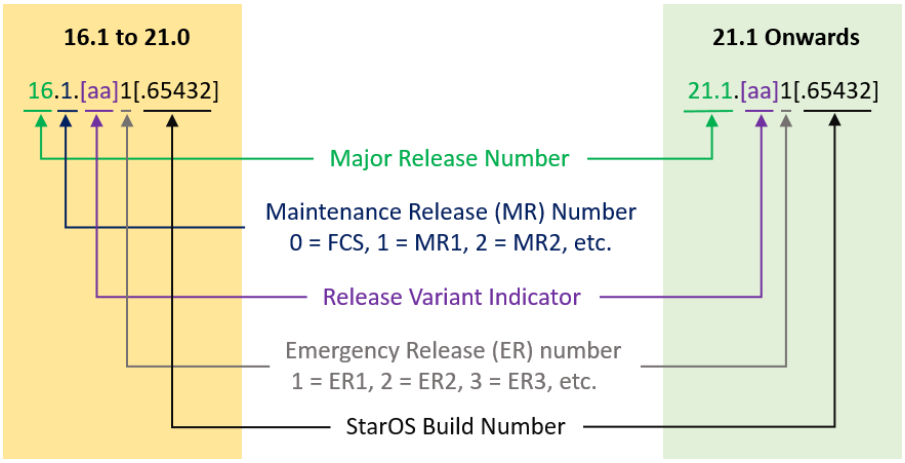
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployme nt releases also differed only in build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

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

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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

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)