Release Notes for StarOS™ Software Version 21.15.0 and Ultra Service Platform Version N6.9.0

First Published: August 29, 2019
Last Updated: August 29, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.14.0 and N6.8.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.15.0 build 72729
Ultra Service Platform ISO	6_9_0-9469
usp-em-bundle*	6.9.0, Epoch 7325
usp-ugp-bundle*	21.15.0, build 72729, Epoch 7324
usp-yang-bundle	1.0.0, Epoch 7290
usp-uas-bundle	6.9.0, Epoch 7385
usp-auto-it-bundle	5.8.0, Epoch 7502
usp-vnfm-bundle	4.5.0.112, Epoch 7291
Ultram Manager	2.7.0, Epoch 831
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in Table 3.

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:

- StarOS: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html
- Ultra Gateway Platform (including the UltraM Solution): https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html
- Ultra Automation Services: https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html
- Virtual Packet Core (including VPC-SI and VPC-DI): https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/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.

Ultra M Hyper-Converged Model Component Version Information

Table 2 - Ultra M Hyper-Converged Model Component Version Information

HW	SW	6.3	6.4	6.5	6.6	6.7	6.8	6.9
	StarOS	69977	70597	70741	71244	71540	72257	72729
	ESC	4.2.0.74	4.3.0.121	4.3.0.121	4.4.0.88	4.4.0.88	4.5.0.112	4.5.0.112
	RH Kernel	7.5	7.5	7.5	7.5	7.5	7.5	7.5
	OSP	10	10	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.
	BIOS	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)

HW	SW	6.3	6.4	6.5	6.6	6.7	6.8	6.9
UCS C240 M4S SFF (NFVI)	CIMC (BMC)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)
	MLOM	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)
C2960XR-48TD-I (Manage-ment)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5
C3850-48T-S (Manage-ment)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

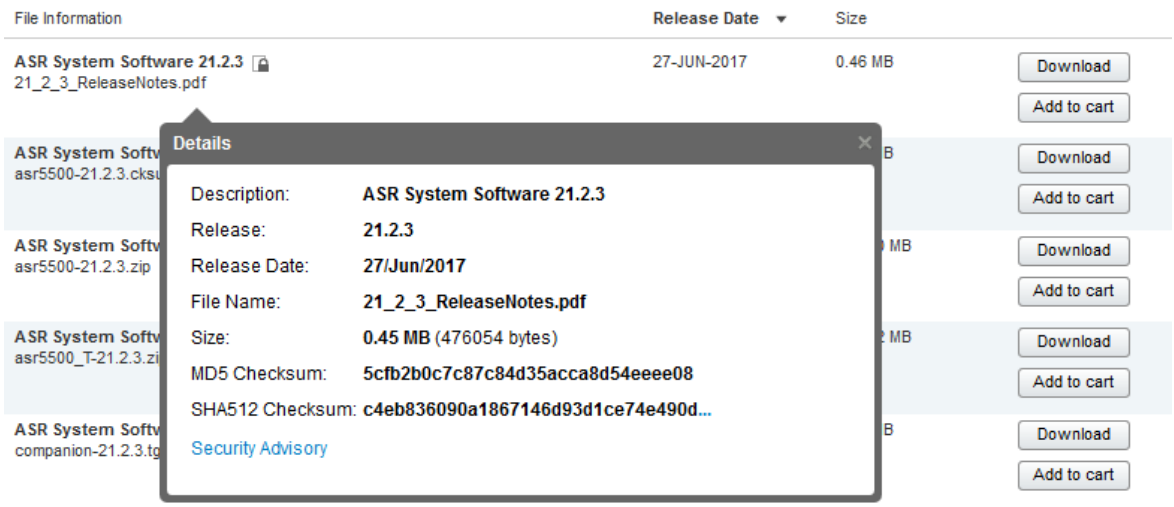
Firmware Updates

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 3 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 3.

Table 3 - 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 4 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvo45414	[BP-CUPS] sx-invalid-response seen when dynamic rule installed after predefined rule and sesMgr kill	cups-cp
CSCvq53786	[BP-CUPS]- sxfail-opr-revert-info session disconnects seen on CP	cups-cp
CSCvq71290	[BP-CUPS]- sx_tun_fsm_handle_sess_mod_rsp_msg()	cups-cp
CSCvq83408	[BP-CUPS]- sessmgr_pgw_cups_detect_active_sx_trans()- pureP	cups-cp
CSCvq83703	[BP-CUPS]- sgwdrv_send_epsb_status_to_smgr()	cups-cp
CSCvq88658	[BP-PLT-CUPS]- iftask_sigusr1_signal_handler()	cups-cp
CSCvq94578	[BP-CUPS]-Invalid/unhandled PDN event <SGWDRV_PDN_EVT_S1_ERROR_IND>	cups-cp
CSCvq94585	[BP-CUPS]-snx_sgw_driver_handle_abort_pdn_req()	cups-cp
CSCvq95227	[BP-CUPS]-SX_MODIFY_REQ failed for Trans: for Current Proc Type: SMGR_PGW_SX_MODIFY_REQ	cups-cp
CSCvq95238	"[BP-CUPS]-For a UE or Admin initiated Deddicated bearer deletion, the PGW trans info is not valid"	cups-cp
CSCvr03232	"[BP-CUPS]: For collapsed call, DDN is getting initiated with incorrect bearer id and arp"	cups-cp
CSCvr05634	[BP-CUPS]-SMGR_PGW_SX_MODIFY_REQ due to last_scheduled_proc_type: SMGR_PGW_BEARER_CMD_NONE	cups-cp
CSCvp45360	[PLT-CUPS-VPP] VPP crash while bringup of 18 vcpu UP with 14 vpp worker threads	cups-up
CSCvq35024	[BP-CUPS]:sessmgr error:Misc Error:Callline invalid or in invalid state for sending checkpoints	cups-up

Bug ID	Headline	Product Found*
CSCvq64442	[BP-CUPS] Subscriber pkt drop stats not updated to sessmgr from VPP on call clear.	cups-up
CSCvq64765	[BP-CUPS] HTTP EDR: one packet for HTTP flow is reported in flow-edr instead of HTTP EDR.	cups-up
CSCvq67869	[BP-CUPS] ULI attribute is not correct in EDR when ECGI is sent in ULI after UP ICSR Switchover.	cups-up
CSCvq71873	[BP-CUPS]- sessmgr_uplane_cleanup_pdr()	cups-up
CSCvq88630	[BP-CUPS]-error- urr Rule Chkpt not exist - urr_element deletion failed	cups-up
CSCvq94592	[BP-CUPS]-uplane_drv_handle_events_from_egtpu_app()	cups-up
CSCvr03672	[BP-CUPS]- egtpu_process_invalid_evt()	cups-up
CSCvo47244	[BP-CUPS] Discrepancy in dropped packet count statistics after Gy quota exhausted	cups-up
CSCvq93693	MME config update not happening on reload chasis applying enb-goup config	mme
CSCvr07661	MME: On unplanned active card migration mme-config-updates are not happening properly	mme
CSCvr08929	sessmgr restart seen on mme_app_fill_delete_sess_req	mme
CSCvq63005	Gbmgr restart seen on gbmgr_rx_gns_pdu	staros
CSCvq87098	[UPF-SVI] QOS not being applied evenly across all calls with static rulebase	upf
CSCvr00066	[UPF]: VPP restart during application of day-1 config	upf
CSCvq82622	[UPF SVI] user-plane-service stats total dropped byte count is 0 even though packets are dropped	upf
CSCvr06501	Deactivate of PCRF NSD fails	usp-uas
* 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 5 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvq46467	[BP-CUPS]-egtpc_handle_user_sap_event()sgwdrv_check_if_paging_can_start_now_for_intf()	cups-cp

Bug ID	Headline	Product Found*
CSCvq71245	[BP-CUPS]-egtpc_handle_user_sap_event()sgwdrv_check_if_paging_can_start_now_for_intf()	cups-cp
CSCvq77475	[BP-CUPS]- egtpc_handle_user_sap_event() sgwdrv_pdn_fsm_st_handle_disconnecting_evt_delete_sess_cfm	cups-cp
CSCvq88619	[BP-CUPS]-snx_sgw_driver_process_query.isra.133()	cups-cp
CSCvq94571	[BP-CUPS]-Invalid/unhandled PDN event <SGWDRV_PDN_EVT_ABORT_PROC_CMD>	cups-cp
CSCvq97012	[BP-CUPS]-sgwdrv_fill_sess_info_from_egtpc_temp_pdn_ingress()	cups-cp
CSCvm92957	[BP-CUPS]sessmgr restarts-smc_sxb_sxab_add_estab_req_info_to_trans_info() license expire/call comes	cups-cp
CSCvp37507	[BP-CUPS]: DBResponse not seen after bearer-inactivity and update-bearer collision	cups-cp
CSCvq41923	[BP-CUPS] Stale sessions observed on UP	cups-up
CSCvq49216	CLI support for idle timeout value under pdn-instance on UP is currently not available	cups-up
CSCvq64765	[BP-CUPS] HTTP EDR: one packet for HTTP flow is reported in flow-edr instead of HTTP EDR.	cups-up
CSCvo27558	sessmgr Assertion failure in egtpc_handle_user_sap_event	mme
CSCvq03879	Single-registration-indication flag not set in case of 4G->3G->4G PS-HO	mme
CSCvq63501	MME does not send MME Config Update after active SF card migration	mme
CSCvp31108	BGP Neighbor limit of 64 per context is not enforced.	pdn-gw
CSCvp37370	[BP-ICUPS]: After enabling VPP the ttl-excd KPI rate of change spiked.	pdn-gw
CSCvp90947	PGW QCI 5 Bearer Active higher then total Bearer Active	pdn-gw
CSCvq39415	StarOS (21.9) adds "0" in "flow end-condition handoff " inside rulebase config	pdn-gw
CSCvp71457	Cisco SGW restart observed while receiveing invalid Create Bearer Req from PGW	pdn-gw
CSCvq02374	sn_diabase_conn_proxy_write() sessmgr crash	pdn-gw
CSCvq35918	Assertion failure at sess/smgr/sessmgr_hi_li.c	pdn-gw
CSCvp51122	Dynamic Dictionary for suppressing "3GPP-GPRS-Negotiated-QoS-Profile" AVP in Gy dcca	pdn-gw
CSCvp10373	sessmgr restart on function acs_dns_parse	sae-gw
CSCvq22882	Sessmgr restart while static IP address allocation	sae-gw
CSCvq28432	abnormal increment of diameter error 3002 messages over Gx Interface	sae-gw
CSCve02630	sessmgr assertion in s4_sn_dp_network_process_peer_setup_req_evt_in_srns_begun	sgsn

Bug ID	Headline	Product Found*
CSCvq76538	Cisco SGW restart observed during Downlink Data notfication	sgw
CSCvk33338	BGP packets going out of the PGW are with incorrect QOS marks	staros
CSCvq03193	starOS and esxi 6.7: networking broken on Rx jumbo frames	staros
CSCvq23678	ASR5500 - Limit file size of tcam_cmds.txt	staros
CSCvq46641	AFIO is leaking a file descriptor whenever it collects a register dump from a device	staros
CSCvn01954	Not possible to request the buffering from sessmgr where the index is > 255	staros
CSCvq86261	active_slave is not switching for bonded interface when interface is shut on leaf	usp-uas
CSCvq34195	zk missing info in /config/vnfs/ and /oper/vnfs/	usp-uas
CSCvq48606	EM: Increse the ncs.service boot time	usp-uas
CSCvq59459	failed to deactivate UAS NSD in multivnf setup due to instance name mismatch when _ in nsd name	usp-uas
CSCvp46347	update-sw RPC does not verify EM NCS HA state	usp-uas
CSCvm98393	confdmgr-0: usp_get_card_slot_id: Failed to read card-id	usp-usf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

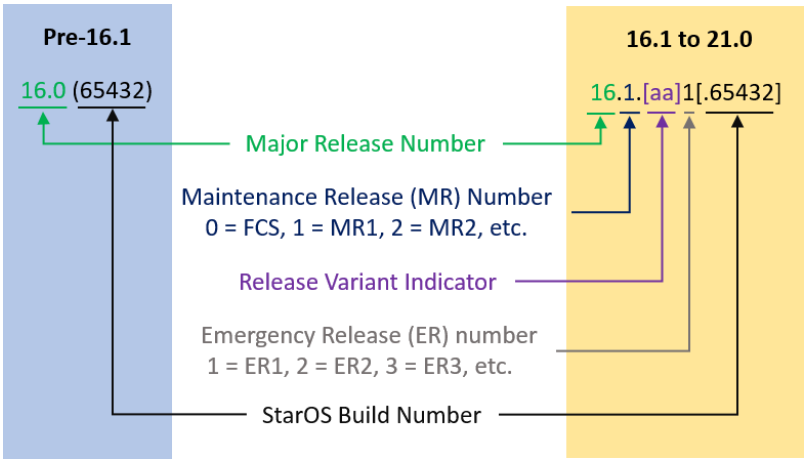
StarOS Version Numbering System

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.

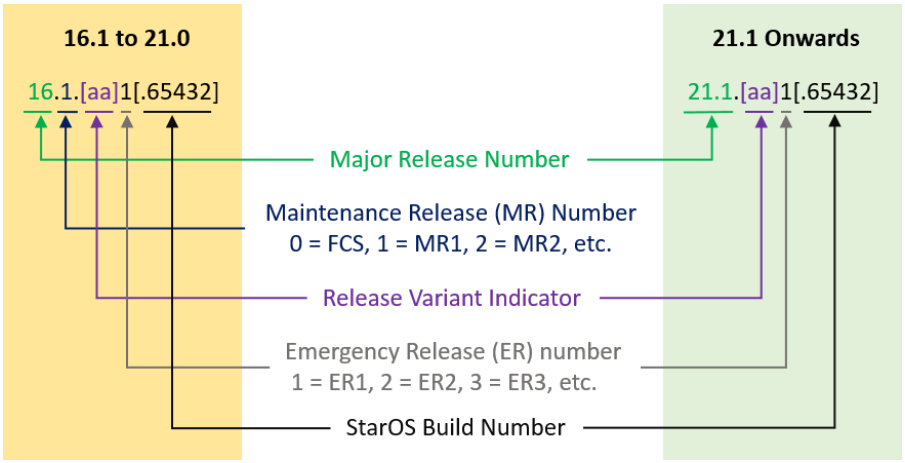
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 6 provides descriptions for the packages that are available with this release.

Table 6 - 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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		

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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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 7 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 7 for descriptions of the specific bundles.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 7 - 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)