Release Notes for StarOS™ Software Version 21.12.0 and Ultra Service Platform Version N6.6.0

First Published: February 14, 2019
Last Updated: February 14, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.11.0 and N6.5.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.12.0 build 71244
Ultra Service Platform ISO	6_6_0-8006
usp-em-bundle*	6.6.0, Epoch 5879
usp-ugp-bundle*	21.12.0, build 71244, Epoch 5906
usp-yang-bundle	1.0.0, Epoch 5784
usp-uas-bundle	6.6.0, Epoch 5967
usp-auto-it-bundle	5.8.0, Epoch 5996
usp-vnfm-bundle	4.4.0.88, Epoch 5785
USP RPM Verification Utilities	6.6.0
* 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	6.1	6.2	6.3	6.4	6.5	6.6
	StarOS	68897	69296	69977	70597	70741	71244
	ESC	3.1.0.145	4.0.0.104	4.2.0.74	4.3.0.121	4.3.0.121	4.4.0.88
	RH Kernel	7.3	7.4	7.5	7.5	7.5	7.5
	OSP	10	10	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.
UCS C240 M4S SFF (NFVI)	BIOS	3.0(3c)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(3e)	3.0(4a)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)
	MLOM	4.1 (3a)	4.1 (3a)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)

HW	SW	6.1	6.2	6.3	6.4	6.5	6.6
C2960XR-48TD-I (Management)	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
	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
C3850-48T-S (Management)	Boot Loader	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
Nexus 93180-YC-EX (Leafs)	BIOS	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)
Nexus 9236C (Spines)	BIOS	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)

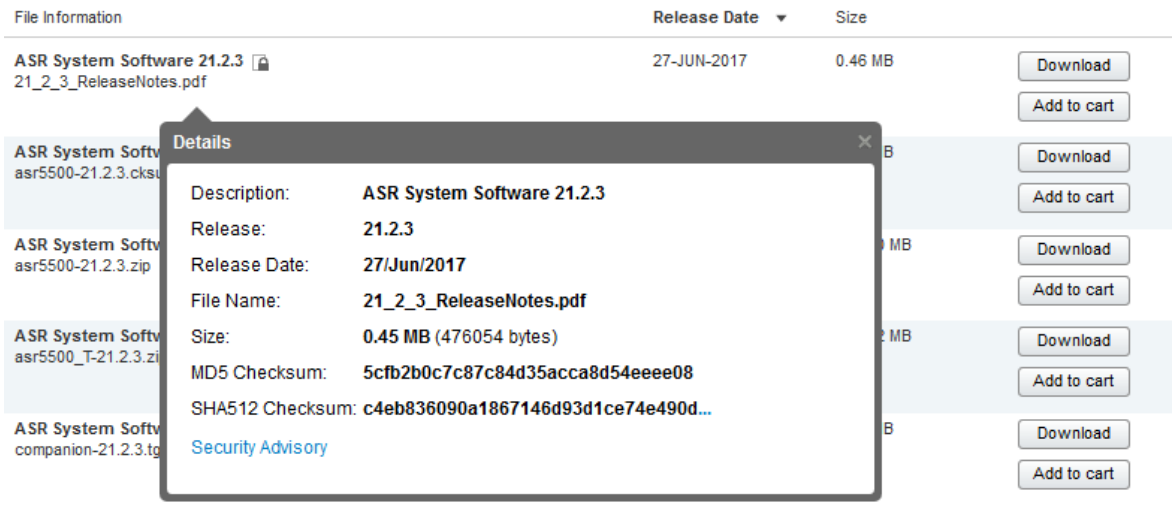
Firmware Updates

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*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvn63100	[BP-CUPS] Assert at saegwdrv_ue_fsm_st_active_evt_snx_line_callstate()	cups-cp
CSCvn80152	[BP-CUPS] Observing new IE Interface: SXa wrongly sent in PFCP Heartbeat Request/Response	cups-cp
CSCvn44898	[PLT-CUPS-VPP] : TCP Flows are not getting cleared after FIN is received	cups-up
CSCvn75110	[BP-CUPS] High memory utilization by sessmgr - probable memory leak	cups-up
CSCvo07207	[BP-CUPS] sessctrl restart in UP	cups-up
CSCvn51661	[BP-CUPS-VPP][ICUPS]Sessmgr 99% utilization for single UE 4Gbps Tput test	cups-up
CSCvo26369	[MME] ETWS - Missing IE values under WRWR/STOP Warning Indication Messages	mme
CSCvo15422	mmemgr task restart due to a segmentation in S1ap	mme
CSCvn55676	[BP-CUPS]:Uplink Stream remain in Config state after Flow status change	pdn-gw
CSCvo18335	[BP-ICUPS]:vpp restart at fapi_module_client_clear on call model run	pdn-gw
CSCvo18360	[BP:ICUPS]:Sessmgr restart at fapi_stream_request() on call model run	pdn-gw
CSCvo19406	[BP:ICUPS]:sessmgr restart on clib_bihash_add_del_16_8_32() on call model run	pdn-gw
CSCvo27235	[BP-ICUPS]: vpp_main stuck in warn state	pdn-gw
CSCvo27865	[BP-ICUPS]: High Speed UE Gy record and call stats data not matching	pdn-gw
CSCvo31100	[BP-ICUPS]X3 table entries absent post DMX migration	pdn-gw
CSCvo32182	[BP-ICUPS]: LI intercept failures on HSLI after ICSR switchover	pdn-gw
CSCvo32237	[BP-ICUPS]: some UDP streams going to passive post ICSR switchover	pdn-gw
CSCvn75072	[BP:ICUPS]:Sessmgr restart@fapi_tp_process_incoming_local_row_req on DPC2 card reboot.	pdn-gw
CSCvo30174	[BP-ICUPS]Unable to get over 4.3 Gbps on HSLI without fifo Q full on threads	pdn-gw
CSCvo35584	pct_bearerplane smoke2test bp_mindboglrs rne-approved	pdn-gw
CSCvo32889	[BP-ICUPS]:sessmgr 0 error fastpath_stream_add(): Stream [Ver: 0, locus: 2, client_id: 8, stats_tabl	sae-gw
CSCvi12541	bfdlc facility instances in warn state on active and standby chassis	sae-gw
CSCvn73574	[BP-ICUPS]:sn-charge-volume in rulematch EDR is counting dropped HTTP resp pkt	sae-gw
CSCvo31408	saegw-service stats not updating for CSRsp denied due to license exceeded	sae-gw
CSCvn94523	F2725: Rab Rel Response counters are not pegged	sgsn

Bug ID	Headline	Product Found*
CSCvo27835	[BP-ICUPS-saegw-DPC2]: HSLI - intercept failures observed due to tx fifo full	staros
CSCvb01503	'show ip route' CLI command causes MemoryWarn snmp trap in qVPC	staros
CSCvn79019	[BP-ICUPS] Streams are not getting recovered after Planned DPC2 Migration with 5g calls	staros
CSCvo04967	StarOS cannot assign multiple IPv6 address for diameter peer	staros
CSCvn81354	EM triggers the deployment of 1 CF only - intermittent and occurances started Dec 14	usp-uas
CSCvo08737	ETSI MANO: EM does not handle service start and service stop	usp-usf
CSCvo20436	Descriptor version and version fields is displayed as unknown	usp-usf
* 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*
CSCvn85625	[CUPS]Calls disconnected with reason sx-no-resource when the Max limit of PDR's/FAR's exceeded	cups-cp
CSCvn83904	BP-CUPS Sessmgr restart with stack acsmgr_fill_urrs_for_static_predef_pdr()	cups-cp
CSCvn84860	[BP-CUPS]:No charging params seen, when dynamic rule is installed, followed by predef rule in rar	cups-cp
CSCvo03515	SX association is not coming up with ip pool after ICSR	cups-cp
CSCvk63958	[PLT-CUPS-ICUPS-VPP]Single user performance blocked due to VPP_MAIN is in over state	cups-up
CSCvn55052	[BP-CUPS]: Assertion failure at uplane_drv_fsm_handle_invalid_evt	cups-up
CSCvm47437	[BP-ICUPS]:Analyser/RB statistics are not counting DL dropped offloaded packets.	cups-up
CSCvm57966	[BP-ICUPS] First DL pkt of UDP flow creating stream in passive state instead of active state	cups-up
CSCvn37654	[BP-CUPS] sxdemux proclet restart on Uplane.	cups-up
CSCvn88975	Unexpected QoS mapping between EPC QCI 8 and Pre-Release 8 QoS	ggsn
CSCvh57724	NB-IOT EDRX ptw and edrx-cycle values are wrongly documented in CLI and documentation	mme

Bug ID	Headline	Product Found*
CSCvn41573	HTTP Fraud detected with use HTTP HEAD modification	pdn-gw
CSCvm55782	[BP-ICUPS]:Dynamic Rule flow status change from Discard to Allow All is not working	pdn-gw
CSCvm82106	[BP-ICUPS] : Packets drop seen at vpp for TEP entries marled with DeferDel as yes.	pdn-gw
CSCvm91229	[BP-ICUPS-VPP] : sessmgr restart at fapi_tp_process_incoming_local_row_req() sp=0xffccd588()	pdn-gw
CSCvn10871	PGW not sending AMBR IE to SGW/MME when AMBR is 0/0kbps	pdn-gw
CSCvn28046	[BP-ICUPS]:streams stuck in passive state in case of 2g to lte and 3g to lte handover scenario	pdn-gw
CSCvn39767	Unexpected session manager restart- _do_acs_usertcp_event_handler()	pdn-gw
CSCvn68072	[BP:ICUPS]:Multiple SMU-FAPI: FAPI_REQUEST_ROW_DELETE_C failed sessmgr error logs	pdn-gw
CSCvn72386	[BP-ICUPS] VPP main stuck in over state after ICSR	pdn-gw
CSCvn77706	Migration to DPC2 card resulted in RAR timeouts	pdn-gw
CSCvn81906	[BP-ICUPS] after ICSR egtpu 142001 error Inline CUPS API to Onload Offload Traffic failed	pdn-gw
CSCvn82035	[BP:ICUPS] sesmgr restart at acsmgr_deallocate_call_obj()	pdn-gw
CSCvn82503	[BP-ICUPS] [sessmgr 10699 Misc Error: Was unable to set thresholds at VPP for EBI, error code 5	pdn-gw
CSCvn91605	[BP-ICUPS] ICSR fastpath_row_read(): returned error 0x80002001 seen on STANDBY	pdn-gw
CSCvn97839	Threshold process goes into warn state because of memory	pdn-gw
CSCvo07828	[BP-ICUPS] : Fastpath LI: LI deactivation not working	pdn-gw
CSCvo07939	[PLT-ICUPS] TCP connection to LI servers doesn't get re-established	pdn-gw
CSCvo20343	[BP-ICUPS]: VPP not offloaded for the session post ICSR switchover	pdn-gw
CSCvm65884	PGW-Around 5% increase in sessmgr memory in 21.11.M0.70658 wrt 21.9.M0.69679 baseline CEPS test	pdn-gw
CSCvn33912	PGW sends Update Bearer Request with unknown filters in TFT	pdn-gw
CSCvn69328	BP-ICUPS : After ICSR switchover, sessions get randomly disconnected due to Idle-Inactivity-timeout	sae-gw
CSCvo01679	[BP-ICUPS-saegw-DPC2]: NPU usage shows 100%, 4 vpp threads unutilized	sae-gw
CSCvk52997	Sessmgr restart while sending fragmented packets out after timeout	sae-gw
CSCvo25473	[BP-ICUPS]Post icsr HTTP flows are not being offloaded.	sae-gw
CSCvk43515	Assertion failure at sm_rab_mgmt	sgsn

Bug ID	Headline	Product Found*
CSCvk45571	sessmgr restart function: sessmgr_gprs_process_sub_session_idle()	sgsn
CSCvj87023	SM fail due to Assertion failure at egtpc_handle_context_ack_evt	sgsn
CSCvn33852	SGSN does not process Re-transmitted Attach Request while waiting for IMEI-Response	sgsn
CSCvk10196	SM fail due to Fatal Signal at sm_gen_s4_prepare_remote_handoff_cfm	sgsn
CSCvn23275	[PLT-ICUPS] Both DPC2 rebooted upon planned migration	staros
CSCvn71225	[PLT-ICUPS] Segmentation fault with DPC Migration	staros
CSCvm98426	[PLT-ICUPS-VPP] Not able to send fragmented packet through VPP.	staros
CSCvn51288	[BP:ICUPS]:sessmgr in warn/over state with call model longivity	staros
CSCvn67152	VPC-DI/XL710: Fix port statistic collection time intervals.	staros
CSCvn72416	[PLT-ICUPS] vpp restart followed by npumgr restart with background callmodel.	staros
CSCvm96218	ASR5K device sends wrong objects for the traps with ifIndex 1343, 1344, 1345, 1346.	staros
CSCvn94836	VPC-DI: iftask double count for di_tx traffic	staros
CSCvn81354	EM triggers the deployment of 1 CF only - intermittent and occurances started Dec 14	usp-uas
***** Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

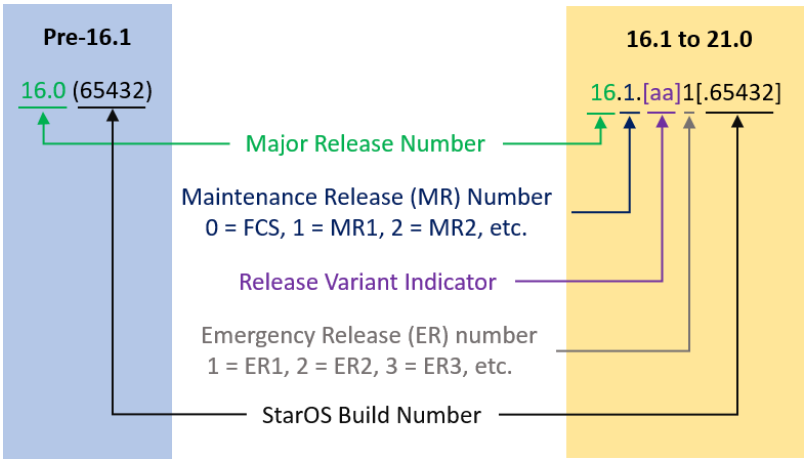
StarOS Version Numbering System

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.

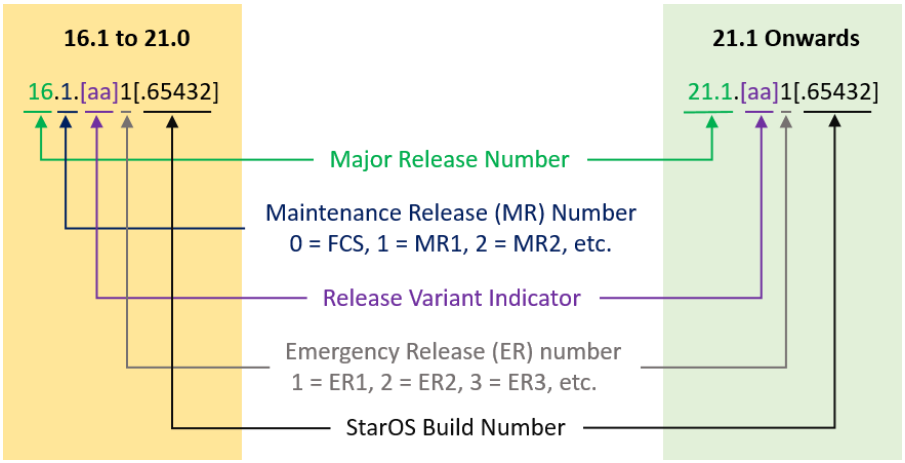
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

© 2019 Cisco Systems, Inc. All rights reserved.