Release Notes for StarOS™ Software Version 21.13.0 and Ultra Service Platform Version N6.7.0

First Published: March 28, 2019
Last Updated: March 28, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.12.0 and N6.6.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.13.0 build 71540
Ultra Service Platform ISO	6_7_0-8441
usp-em-bundle*	6.7.0, Epoch 6274
usp-ugp-bundle*	21.13.0, build 71540, Epoch 6332
usp-yang-bundle	1.0.0, Epoch 6237
usp-uas-bundle	6.7.0, Epoch 6393
usp-auto-it-bundle	5.8.0, Epoch 6449
usp-vnfm-bundle	4.4.0.88, Epoch 6238
USP RPM Verification Utilities	6.7.0
* 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	6.7
	StarOS	68897	69296	69977	70597	70741	71244	71540
	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	4.4.0.88
	RH Kernel	7.3	7.4	7.5	7.5	7.5	7.5	7.5

HW	SW	6.1	6.2	6.3	6.4	6.5	6.6	6.7
	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.	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)	3.0(4a)
	CIMC (BMC)	3.0(3e)	3.0(4a)	3.0(4d)	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)	4.1 (3f)
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	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 (Management)	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)

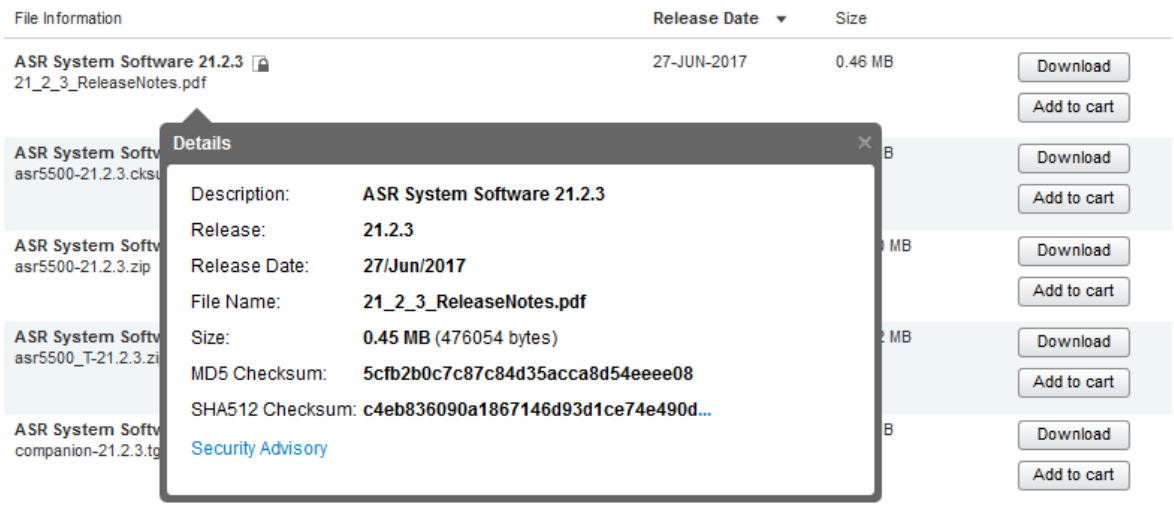
Firmware Updates

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*
CSCvi53376	[BP-CUPS]: Session Manager reload at smgr_uplane_config_rule_options on Cisco PGW	cups-up
CSCvo50367	[PLT-CUPS-VPP] Pure-S or Pure-P packets not getting counted with ipv6 on S5-U transport	cups-up
CSCvo48870	[PLT-CUPS]Calls are not coming up after adding new UP when new UP doesn't get any chunks	cups-up
CSCvo55798	[BP-CUPS] UP becomes inaccessible abruptly	cups-up
CSCvo72099	[BP-CUPS] SX MH BFD was going down when one of the redundant Gn ports was shut down	cups-up
CSCvo80112	[PLT-CUPS]New chunk allocation to UPs not happening after pool context vpnmgr recovery	cups-cp
CSCvo87716	[BP-CUPS] IP pool chunks not allocated from all IP pools	cups-cp
CSCvo87947	[BP-ICUPS]:serviceCondChange as Normal Release instead of Management Intervention	pdn-gw

Bug ID	Headline	Product Found*
CSCvo89792	[BP-ICUPS]:servers-unreachable CCRU is not going for interim-quota exhaust	pdn-gw
CSCvo93945	[PLT-ICUPS]:vpp restart observed with build load and without any calls	sae-gw
CSCvo98718	'Unknown' session disconnect reasons incremented after DSReq received instead of MBreq in multipdn	sae-gw
CSCvo37441	wrong firewall Ruledef stats shown in 'show active-charging ruledef statistics all firewall wide'.	pdn-gw
CSCvo46856	[BP-CUPS]: SxModiReq/res counter remains 0 in sx-service statistics	cups-cp
CSCvo57995	[PLT-CUPS] : Selective support for ICMP unavailable in VPP	staros
CSCvo85287	[BP-ICUPS] : sessmgr restart observed at sn_msg_arriving_handle()	pdn-gw
CSCvo85755	[PLT-ICUPS] HS-LI-UDP: Uplink packets are not getting intercepted	sae-gw
CSCvo99003	[ICUPS] High CPU observed with mon sub is enabled for a subscriber.	pdn-gw
CSCvo99745	show CLI output shows incorrect AMBR values in LTE 2G/3G LTE on 21.13.M0	sae-gw
CSCvp01304	crash reported on qvpc-di setup. Process - confdmgr Function: confdmgr_fsm_state_wait_p1_handler()	staros
CSCvp11547	[BP-ICUPS-saegw-DPC2]: HSLI IPSEC - Trusted build crashing continuously	staros
CSCvo87872	[BP-ICUPS]: L2 marking: No DL streams created when the l2 mapping table with odd values	sae-gw
* 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*
CSCvo17914	[PLT-CUPS]: vpn_ip_pool_cups_send_chunks_chkpoint_notification	cups-cp
CSCvn80152	[BP-CUPS] Observing new IE Interface: SXa wrongly sent in PFCP Heartbeat Request/Response	cups-cp
CSCvo13488	[BP-CUPS] Sessctrl in 'Over' state with 10k calls	cups-up
CSCvo32286	[PLT:CUPS] VPP forwards VLAN tagged pkt as untagged to NPUSIM	cups-up
CSCvn61157	Memory leak in ipsecmgrs	epdg
CSCvn35566	Assertion failure at sessmgr_ipsg - a new appearance	ipsg
CSCvo55100	clear mme-service statistics not clearing Dual Connectivity with NR Subscribers stats	mme

Bug ID	Headline	Product Found*
CSCvo88008	" MME, Collision Case - E-RAB Mod for NR addition CBReq for VoLTE termination call attempt"	mme
CSCvm97400	Assert at mme_app_fill_s1_bearer_values	mme
CSCvo13661	cc overwrite apn remap is case sensitive	mme
CSCvo15422	mmemgr task restart due to a segmentation in S1ap	mme
CSCvo33689	inter-rat-nnsf mme-codes parameter missing after reload	mme
CSCvn09785	sessmgr crashed after modify ECS configuration	pdn-gw
CSCvo85261	[BP-ICUPS]:sessmgr restart observed at acsmgr_fp_handle_stream_state_change()	pdn-gw
CSCvo93860	BP-ICUPS: ipsecmgr in warn state for HS LI with ipsec	pdn-gw
CSCvg88726	[ICSR] Increase number of Dynamic rule failure logs	pdn-gw
CSCvn57633	P2P plugin automatic rollback	pdn-gw
CSCvo06323	Sessmgr restart at function xdr_acs_show_sfw_rule_info_t()	pdn-gw
CSCvo08450	21.10.1: PGW is adding extra character 19 in MSISDN PCO on CSResp during SIM activation scenario.	pdn-gw
CSCvo17281	aaamgr memory leak due to checkpointing	pdn-gw
CSCvo18926	Interim UDR not generated for Subscriber performing multiple rulebase change	pdn-gw
CSCvo49917	[BP-ICUPS] sessctrl in Over state on 21.12.0.71244 EFT	sae-gw
CSCvo77517	[BP-ICUPS] LTE to 2G to LTE results in 2G speeds on 21.12.3	sae-gw
CSCvo16699	Cisco SAE-GW restart seen if MME is sending HLCOM IE's (feature is deavated on SAE-GW)	sae-gw
CSCvo32889	" [BP-ICUPS]:sessmgr 0 error fastpath_stream_add(): Stream [Ver: 0, locus: 2, client_id: 8, stats_tabl"	sae-gw
CSCvo36105	[BP-ICUPS]: acsmgr 91369 error Error: Client-Server API: Add conneciton request to Dhost failed	sae-gw
CSCvo45264	[BP-ICUPS]: Data is not proper for 5G UE of ipv6 pdntype	sae-gw
CSCvo64893	[saegw-gn] LI interception of calltype saegw does not intercept 2G/3G calls	sae-gw
CSCvo82068	[BP-ICUPS]: 4G sub with NAT44 fragmented traffic NOT getting charged to Dynamic rule	sae-gw
CSCvo69466	[BP-ICUPS] Unable to decode some PGWCDRs on 21.12.3	sae-gw
CSCvo95499	[BP-ICUPS] 21.13.M0 starent.my returns a compilation error for severity2 `starTrapGroup'	sae-gw

Bug ID	Headline	Product Found*
CSCvm74886	bulkstat process restart at PC: [0480526e/X] mgmt_sctrl_add_sgsn_gmm_sm_stats()	sgsn
CSCvn77932	SGSN EDR header does not have EOL character	sgsn
CSCvo00288	Cisco SGW Restart observed on Standby ICSR chassis	sgw
CSCvm93753	MIB Syntax Errors in 21.8.1 (69429) and 21.9.1 (70183)	staros
CSCvn22364	MIB SRP IPv6 SNMP Traps in 21.8.1 (69429) and 21.9.1 (70183) Not Decoded Correctly.	staros
CSCvo37389	sessmgr/diamproxy mapping mismatch after DPC migration	staros
CSCvn00287	Receiving snmp 22012 Unsupported Platform Logs In Virtual Gateway	staros
CSCvo04967	StarOS cannot assign multiple IPv6 address for diameter peer	staros
CSCvo29918	Wrong echo-max-retransmissions value when not explicitly configured	staros
CSCvo08737	ETSI MANO: EM does not handle service start and service stop	usp-usf
***** Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

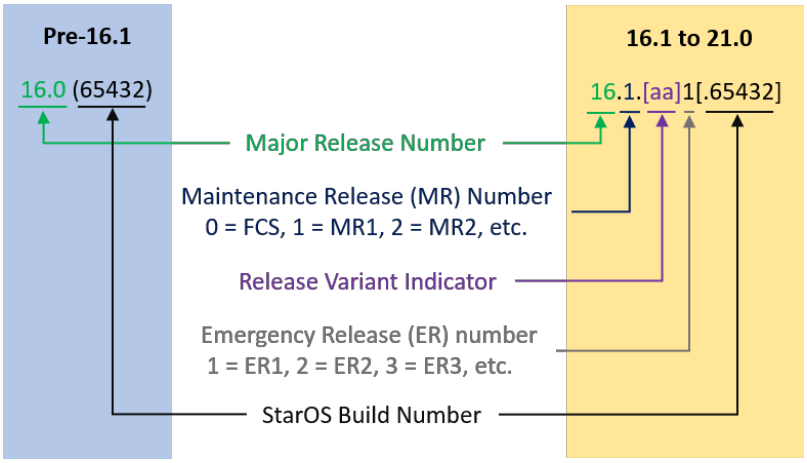
StarOS Version Numbering System

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.

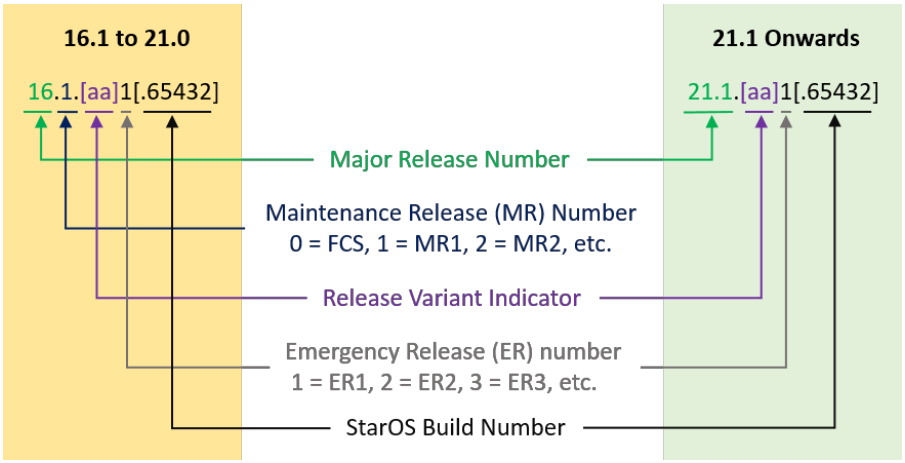
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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

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

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