



# Release Notes for StarOS™ Software Version 21.12.13 and Ultra Service Platform Version N6.6.5

**First Published:** Nov 25, 2019

**Last Updated:** Nov 25, 2019

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on StarOS release 21.12.12 and USP release N6.6.4. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

## Release Package Version Information

**Table 1 - Release Package Version Information**

Software Packages	Version
StarOS packages	21.12.13 build 73564
Ultra Service Platform ISO	6_6_5, Epoch 10007
usp-em-bundle*	6.6.0, Epoch 7551
usp-ugp-bundle*	21.12.13, build 73564, Epoch 7806
usp-yang-bundle	1.0.0, Epoch 5784
usp-uas-bundle	6.6.0, Epoch 7070
usp-auto-it-bundle	5.8.0, Epoch 5996
usp-vnfm-bundle	4.4.0.88, Epoch 5785
ultram-manager RPM*	2.4.0, Epoch 333
USP RPM Verification Utilities	6.6.5
* 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	73564
	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 <b>NOTE:</b> OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 <b>NOTE:</b> OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.

## Installation and Upgrade Notes

HW	SW	6.1	6.2	6.3	6.4	6.5	6.6
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)
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

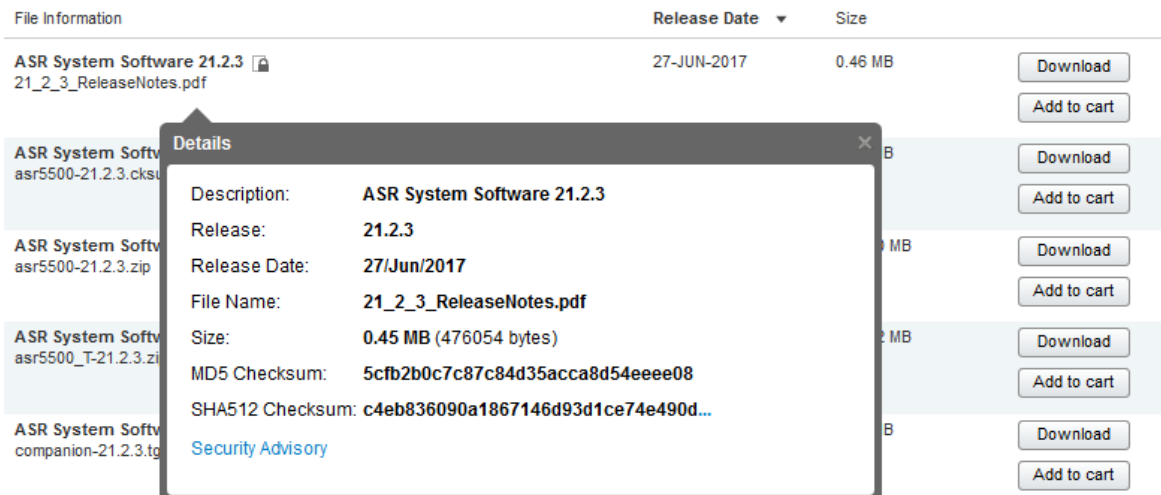
There are no firmware upgrades required for this release.

## 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.

Installation and Upgrade Notes



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  <pre>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>
Apple MAC	Open a terminal window and type the following command  <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
Linux	Open a terminal window and type the following command  <pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
<b>NOTES:</b>	
<i>&lt;filename&gt;</i> is the name of the file.	
<i>&lt;extension&gt;</i> 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.

## Open Bugs in this Release

## 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
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
CSCvn75110	[BP-CUPS] High memory utilization by sessmgr - probable memory leak	cups-up
CSCvo01375	[CUPS] VPP restart observed with stack libvlib.so.0/unix_cli_file_welcome_timer()	cups-up
CSCvo07207	[BP-CUPS] sessctrl restart in UP	cups-up
CSCvo48775	MME: MEC - Inter-MME S1 HO trigger unexpected detach	mme
CSCvo55100	clear mme-service statistics not clearing Dual Connectivity with NR Subscribers stats	mme
CSCvr23734	[mme]- congestion-actions triggers not applied during congestion_post reload	mme
CSCvs15514	[MME]- Bulkstats_tai timeout traps not generating	mme
CSCvo15422	mmemgr task restart due to a segmentation in S1ap	mme
CSCvq93693	MME config update not happening on reload chassis applying enb-goup config	mme
CSCvo85261	[BP-ICUPS]:sessmgr restart observed at acsmgr_fp_handle_stream_state_change()	pdn-gw
CSCvo20908	[PLT-ICUPS-VPP]:VPP Main in memory over state	pdn-gw
CSCvo31100	[BP-ICUPS]X3 table entries absent post DMX migration	pdn-gw
CSCvo32237	[BP-ICUPS]: some UDP streams going to passive post ICSR switchover	pdn-gw
CSCvp05331	[BP-ICUPS] PGWCDR is not generated with dynamic DDL config	pdn-gw
CSCvp37370	[BP-ICUPS]: After enabling VPP the ttl-excd KPI rate of change spiked.	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

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvo37441	wrong firewall Ruledef stats shown in 'show active-charging ruledef statistics all firewall wide'.	pdn-gw
CSCvo49917	[BP-ICUPS] sessctrl in Over state on 21.12.0.71244 EFT	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 connecton request to Dhost failed	sae-gw
CSCvo45264	[BP-ICUPS]: Data is not proper for 5G UE of ipv6 pdntype	sae-gw
CSCvo82068	[BP-ICUPS]: 4G sub with NAT44 fragmented traffic NOT getting charged to Dynamic rule	sae-gw
CSCvi12541	bfdlc facility instances in warn state on active and standby chassis	sae-gw
CSCvo31408	saegw-service stats not updating for CSRsp denied due to license exceeded	sae-gw
CSCvo47301	[BP-ICUPS]Quota_ Exhaust not triggered for pipelined request packet	sae-gw
CSCvs17393	Multiple Instances of sessmgr restart observed in egtpc_get_ebi_info_from_pdu()	sgsn
CSCvs18939	Multiple Instances of sessmgr restart observed in sgsn_app_allocate_svc_req_cb()	sgsn
CSCvp10744	[BP-ICUPS] SGW CDR shows double value in dataVolumeGPRSDownlink for buffered data after Re-establish	sgw
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
CSCvo20944	[BP-ICUPS]: starOS CLI commands are NOT getting logged into configured syslog	staros
CSCvp47435	ipv4 reassembly timeout - vpp restart	staros
CSCvr49515	ASR5500   21.12.9(72306)   PGW   Frequent Bulkstat Restart	staros
CSCvn81354	EM triggers the deployment of 1 CF only - intermittent and occurrences started Dec 14	usp-uas
CSCvo84219	multi-vnfd generation fails when using different pools of same net	usp-uas
CSCvo95462	Same virtual_router_id for all UEM deployments	usp-uas
CSCvr40956	EM freeze leading to stuck vnfm proxy	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*
CSCvr09625	collision e-rab setup and TAU leading to bearer release	mme
CSCvq77876	Assertion Failure in sn_aaa_session_set_user_data()	mme
CSCvr10617	Enh: add warning when TAI stat collection takes too long and trap when beyond	mme
CSCvq42650	MME sends a wrong IPv6 transport address in ERAB setup	mme
CSCvp22149	"MME, Inter-TAU or S1 HO - EGTP_CAUSE_MANDATORY_IE_INCORRECT from new MME"	mme
CSCvp43902	EPC MME; GBR bearer preservation by Inter-RAT redirection cause in UE context release	mme
CSCvq23483	MME: Sessmgr's memory over usage across multiple STAROS instances	mme
CSCvq63501	MME does not send MME Config Update after active SF card migration	mme
CSCvr43249	Framed route not added even when Radius Authentication Server sends Framed Route AVP towards PGW	pdn-gw
CSCvq87421	Assertion failure at ./sess/aaamgr/aaamgr_data_api	sgsn
CSCvr00128	Assertion failure at sess/aaamgr/aaamgr_api.c	sgsn
CSCvr05830	session manager restarts during egtp handling	sgsn
CSCvr23777	sessmgr assert - Invalid Event NTKW-REMOTE-HANDOFF-REQUEST from SM-APP	sgsn
CSCvq63005	Gbmgr restart seen on gbmgr_rx_gns_pdu	sgsn
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

## Operator Notes

### StarOS Version Numbering System

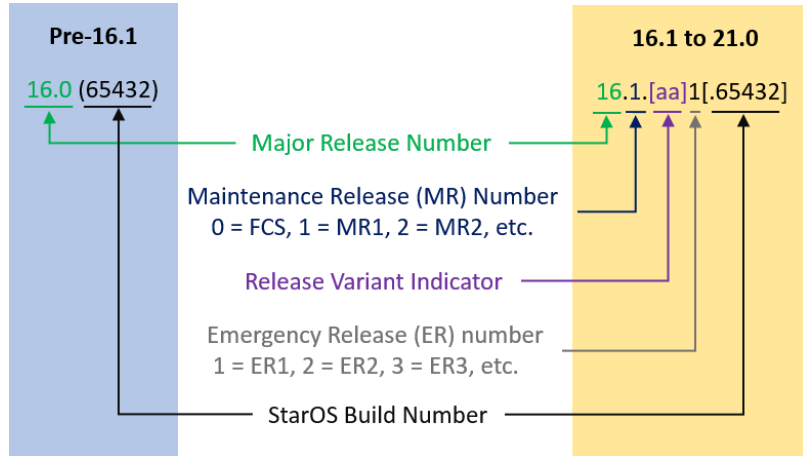
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

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.

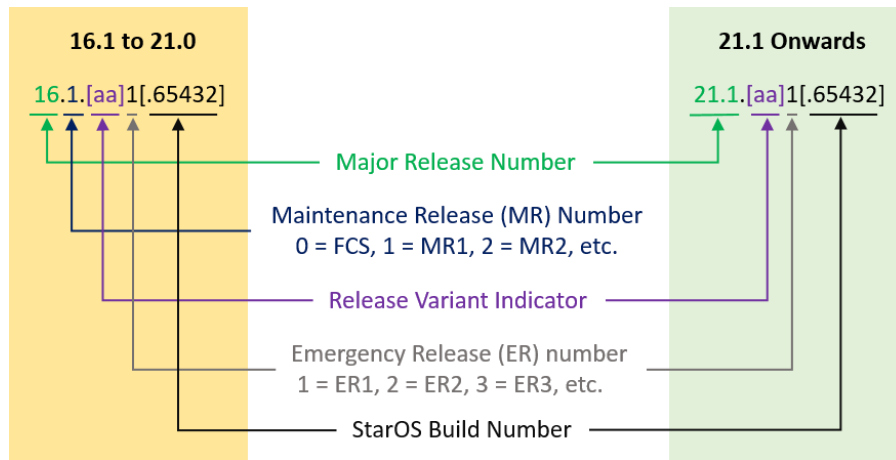
Operator Notes

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
<b>ASR 5500</b>		



## Operator Notes

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
asr5500- <release>.zip	asr5500- <release>.bin	Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
asr5500_T- <release>.zip	asr5500_T- <release>.bin	Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
<b>StarOS Companion Package</b>		
companion- <release>.zip	companion- <release>.tgz	<p>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.</p> <p>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.</p>
<b>VPC-DI</b>		
qvpc-di- <release>.bin.zip	qvpc-di- <release>.bin	<p>Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di_T- <release>.bin.zip	qvpc-di_T- <release>.bin	<p>Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di- <release>.iso.zip	qvpc-di- <release>.iso	<p>Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>

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

## Operator Notes

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	<p>Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
<b>VPC-SI</b>		
qvpc-si- <release>.bin.zip	qvpc-si- <release>.bin	<p>Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si_T- <release>.bin.zip	qvpc-si_T- <release>.bin	<p>Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si- <release>.iso.zip	qvpc-si- <release>.iso	<p>Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si_T- <release>.iso.zip	qvpc-si_T- <release>.iso	<p>Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si-template- vmware- <release>.zip	qvpc-si-template- vmware- <release>.ova	<p>Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>

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

## Obtaining Documentation and Submitting a Service Request

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
usp-<version>.iso		The USP software package containing component RPMs (bundles).  Refer to <a href="#">Table 7</a> for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images.  Refer to <a href="#">Table 7</a> 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](http://www.cisco.com/go/offices).

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

© 2019 Cisco Systems, Inc. All rights reserved.