# Release Notes for StarOS™ Software Version 21.26.h5

**First Published:** April 04, 2023
**Last Updated:** April 04, 2023

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.26.h4.

## Release Package Version Information

**Table 1 - Release Package Version Information**

| Software Packages | Version |
|---|---|
| StarOS packages | 21.26.h5, build 89399 |

## 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 http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html.

## Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

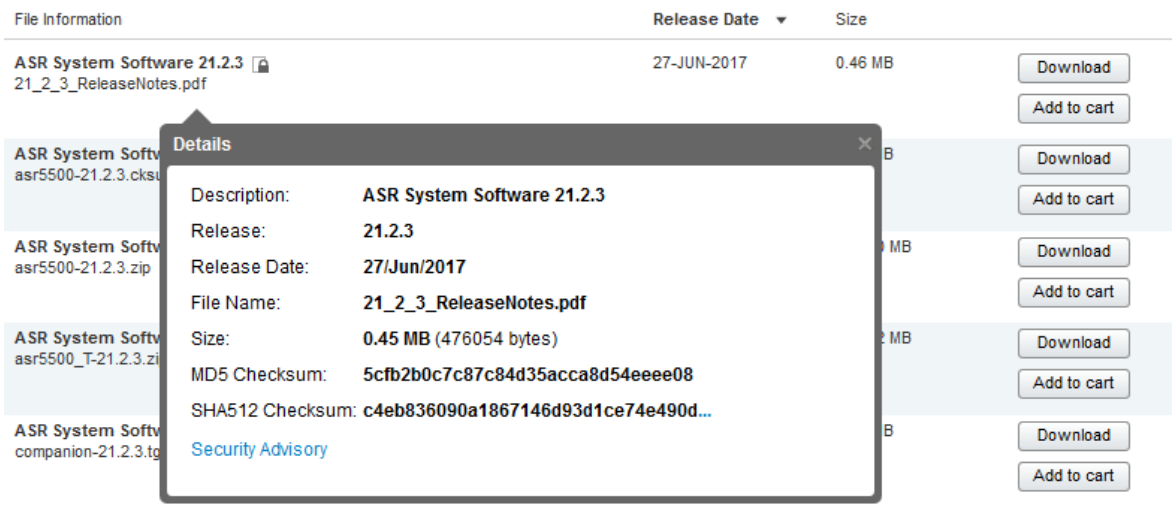
## Firmware Updates

There are no firmware upgrades required for this release.

## Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **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 2 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 2.

**Table 2 - Checksum Calculations per Operating System**

| Operating System | SHA512 checksum calculation command examples |
|---|---|
| Microsoft Windows | Open a command line window and type the following command<br><br>> certutil.exe -hashfile *<filename>.<extension>* SHA512 |
| Apple MAC | Open a terminal window and type the following command<br><br>$ shasum -a 512 *<filename>.<extension>* |
| Linux | Open a terminal window and type the following command<br><br>$ sha512sum *<filename>.<extension>*<br><br>Or<br><br>$ shasum -a 512 *<filename>.<extension>* |
| **NOTES:**<br><br>*<filename>* is the name of the file.<br><br>*<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 3 - Open Bugs in this Release**

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwc83349 | [sgw 140014 error] Failure dispatching event <SNX_MSGTYPE_SGW_ADD_PDN_REQ> during longevity test | cups-cp |
| CSCwe81678 | [cups-cp][21.26.h5.89368][SI] SessMgr Crash at sess/snx/drivers/sgw/sgw_pdn_fsm_util.c:17189 | cups-cp |
| CSCwa83375 | [BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup | cups-cp |
| CSCwb57352 | [CUPS] Sx-Modify containing Usage-Report failed. Cause=64 OffendingIE Type=131 | cups-cp |
| CSCwa16910 | [BP-CUPS] Assertion failure @ sess/sx/sxc/sx_interface.c:235 func sx_handle_user_sap_event | cups-cp |
| CSCvz44140 | [BP-CPUS] mostly all aaamgr goes in warn state while running call model | cups-cp |
| CSCwc95182 | SGW doesn't send DBR/DSR triggered by GTPU path failure | cups-cp |
| CSCwa54600 | [BP-CUPS] Assertion failure @ PC: [08dc3801/X] fill_dyn_chrg_rule_name_info() | cups-cp |
| CSCwc63031 | Sgsn change cdr prints wrong sgsn ip address when performing pureP to Collapsed Handover. | cups-cp |
| CSCwe74646 | sessmgr restart on CUPS CP at function acsmgr_create_nsh_info | cups-cp |
| CSCwc07644 | [BP-CUPS]AF at sess/smgr/sessmgr_gr_sess.c:1368 sessmgr_gr_handle_session_full_checkpoint on standby | cups-cp |
| CSCwd43179 | please also apply the fix of CSCwc95182 to Cause New PDN type due to single address bearer only | cups-cp |
| CSCwc59454 | slow response for new calls to existing apn / ip pool at “push config” and “update ip-pool” | cups-cp |
| CSCwe81062 | CDRs are not sent after unplanned SF card migration | cups-cp |
| CSCwa61385 | Hermes: show ipv6 neighbors vpp has no output in HX | cups-up |
| CSCvz99295 | [CUPS-TACACS-IPSEC] Crypto map is in Incomplete after configuring | cups-up |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwe87573 | [cups-up][21.26.h5.89368] UP crash on SM @ sessmgr_populate_pdr_in_teid_list | cups-up |
| CSCwa98318 | [BP-CUPS] Assertion failure at Function: sn_memblock_memcache_alloc() | cups-up |
| CSCwd70361 | Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23427 | cups-up |
| CSCvw79600 | “loopXX create failed” when recreate VRF on UP. | cups-up |
| CSCwa04551 | [BP-CUPS]:Fatal Signal 6: Aborted Signal from: kernel | cups-up |
| CSCwd10265 | [5GaaS] MME sending wrong destination realm resulting in 3002 from DRA | mme |
| CSCwb09095 | MME shall include Monitoring-Event-Report even when count of UEs is 0. | mme |
| CSCwa39049 | UBR Buffering is partially working | mme |
| CSCwb60734 | Observing SDF Filter decoding failed error in Syslog during IMS call model run | pcf |
| CSCwa44222 | BP-ICUPS: VPP buffer were full while running callmodel when CUSP is enabled | pdn-gw |
| CSCwa52583 | ICUPS : Session Manager restarts on PGW | pdn-gw |
| CSCwe23018 | CLI corruption in the output after running “update active-charging override-control rulebase-config | pdn-gw |
| CSCwa41640 | BP-ICUPS: fragmentation doesn't work properly with CUSP enabled | pdn-gw |
| CSCwe21138 | BP-ICUPS: sessmgr crash : sfw_nat_allocate_port_chunk_from_recovery_list() | pdn-gw |
| CSCwc83287 | [Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression | pdn-gw |
| CSCwe64879 | Bulkstats are reporting high utilization for DATARATE_IPPOOL schema | pdn-gw |
| CSCwa49391 | [BP-CUPS] Traffic Optimization UP stats not getting incremented/decremented properly | pdn-gw |
| CSCvz65453 | [SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN | sae-gw |
| CSCwa40146 | [LI-PGW] Observed un-expected content buffer stats output | sae-gw |
| CSCwd27711 | [UPF-SVI] : Uplane received invalid far id in PDU | smf |
| CSCwa37867 | GRE Tunnel with KA not coming up after Card Migration | staros |
| CSCwd74056 | [UPF] IPv4v6 PDN Data Statistics not updated correctly for packet drops due to flow discard | upf |
| CSCwe59504 | [UPF-SVI]: sessmgr crash at sx_validate_pfcp_message() | upf |
| CSCvy08166 | sx peers not reconnecting after SMF shut/start | upf |
| CSCwe29094 | [UPF-SVI] : Seen Uplane received invalid far id in PDU on task kill | upf |
| CSCwe59457 | [UPF-SVI]: sessmgr crash at sx_tun_fsm_handle_sess_mod_rsp_evt() | upf |
| CSCwe34967 | [UPF-SVI]:Invalid Checksum error in show srp info cli even though there is no mismatch in srp config | upf |
| CSCvz47574 | [UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF | upf |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwb99802 | UPFs sending unexpected Session Event Records (SERs) | upf |
| CSCwe33291 | [UPF-SVI]: Continuous error logs on standby UPF “SMGR ID mismatch during recovery” | upf |
| CSCwe32690 | vpp crash causing UPF reload | upf |
| CSCwe35532 | VPNMGR-INSTANCE 3 MEMORY ISSUE ON ICSR UPF pair | upf |
| CSCwd18400 | configurable CLI for hold-queue-size change to be persistent. | upf |
| * Information in the “Product Found” column identifies the product in which the bug was initially identified. | | |

# Resolved Bugs in this Release

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

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

**Table 4 - Resolved Bugs in this Release**

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwe75230 | CP Tries Updating PDR ID 0x0000 - resulting in Reject and VoLTE Call Drop | cups-cp |
| CSCwe70452 | [CUPS-CP] SessMgr restart while handling response for deletion | cups-cp |
| CSCwd19554 | [BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot | cups-cp |
| CSCwb98378 | Idle-Timer on UP is not reset | cups-up |
| CSCwe32987 | [BP_CUPS] NSH Traffic steering is broken on hermes - 21.26.hx | cups-up |
| CSCwa16073 | F124010: L2 traffic steering instance redundancy issue | cups-up |
| CSCwa30749 | [BP-CUPS]Continuous error logs- 'In smgr_uplane_compare_tcond_cf_policy_id returning false]' | cups-up |
| CSCwb54746 | Sessmgr restarted on UP at uplane_check_modify_copy_orig_ip_packet() | cups-up |
| CSCwc95490 | Assertion failure at sess/sctrl/sessctrl_rcm.c:326-Func-sctrl_config_rcm_service() | cups-up |
| CSCwe53212 | MLX5 Core Driver - missing local and vnfmeth interfaces | cups-up |
| CSCwa61829 | "APN MTU value isn't applied at UP when push config is disabled," | cups-up |
| CSCwc98184 | [CUPS-BP]post-processing flow action redirect-url is not working | cups-up |
| CSCwd46286 | "Gy Server returns RC 5030 causing Assume Positive to kick in, CCR-T will contain USU with all zero" | pdn-gw |
| CSCwd39197 | E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query | pdn-gw |
| CSCwd65441 | E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query | pdn-gw |
| CSCwd29917 | Multihop BFD goes down after static single hop BFD recovery | pdn-gw |
| CSCwe59929 | Billing Impact caused by Gy CCR-T Request Number incorrectly increases after Assume Positive | pdn-gw |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwc80092 | Flows are getting terminated even before the configured flow limit is reached | pdn-gw |
| CSCwd26943 | AA Request sent by PGW with MCC 314 has the User-Name AVP MNC transposed to 024 in the Realm | pdn-gw |
| CSCwb65646 | [S8HR]Malformed packets in IMS signalling/media message | sgw |
| CSCwb75361 | [S8HR] sessctrl restart sessctrl_handle_s8hr_apn_list | sgw |
| CSCwd65439 | Password change option for user in warning period before expiration. | staros |
| CSCwe10556 | [UPF] Flow Idle timing out even thought traffic is seen on fastpath | upf |
| CSCwe60139 | "[UPF]Idletimer is triggered post switchover, even if UE is not in idle state for defined duration." | upf |
| CSCwd50985 | [UPF]UPIR(inactivity report) not handled correctly on UE service activation. | upf |
| CSCwe30498 | "[UPF]Time quota is not reset post UPF 1:1 ICSR, in case new quota is not provisioned." | upf |
| CSCwe12006 | [UPF]:Xheader is not inserted becoz of wrong rule match for concatenated req pkts with 1 req partial | Upf |

# Operator Notes

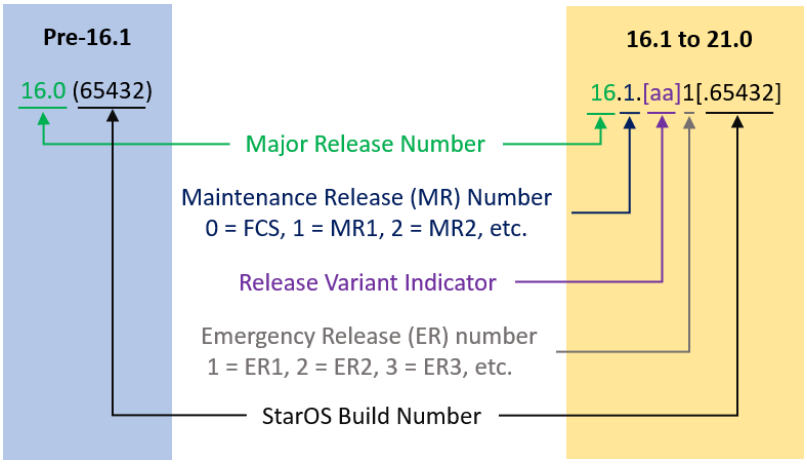
## StarOS Version Numbering System

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.

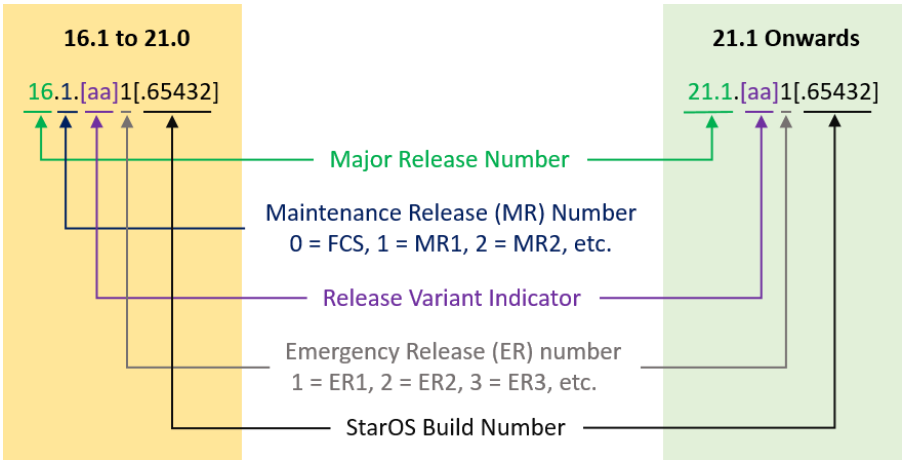
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 4 provides descriptions for the packages that are available with this release.

**Table 4 - Release Package Information**

| In 21.12.0 and later Releases | In pre-21.12.0 Releases | Description |
|---|---|---|
| **ASR 5500** | | |
| asr5500-<release>.zip | asr5500-<release>.bin | Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. |
| asr5500_T-<release>.zip | asr5500_T-<release>.bin | Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. |
| **StarOS Companion Package** | | |
| companion-<release>.zip | companion-<release>.tgz | Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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-<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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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 |
|---|---|---|
| **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.<br><br>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).<br><br>Refer to Table 5 for descriptions of the specific bundles. |
| usp_T-<version>.iso | | The USP software package containing component RPMs (bundles). This bundle contains trusted images.<br><br>Refer to Table 5 for descriptions of the specific bundles. |
| usp_rpm_verify_utils-<version>.tar | | Contains information and utilities for verifying USP RPM integrity. |

**Table 5 - 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)