# Release Notes for StarOS™ Software Version 21.28.mh3

**First Published:** March 15, 2023
**Last Updated:** March 15, 2023

## Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.28.m0. This release note is specific to CUPS User Plane only.

## Release Package Version Information

**Table 1 - Release Package Version Information**

| Software Packages | Version |
|---|---|
| StarOS packages | 21.28.mh3, build 89198 |

## 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.

**Cisco Systems, Inc.**     www.cisco.com

| File Information | Release Date ▼ | Size | |
|---|---|---|---|
| ASR System Software 21.2.3 🔒 21_2_3_ReleaseNotes.pdf | 27-JUN-2017 | 0.46 MB | Download / Add to cart |

**Details** ×

| | | |
|---|---|
| Description: | ASR System Software 21.2.3 |
| Release: | 21.2.3 |
| Release Date: | 27/Jun/2017 |
| File Name: | 21_2_3_ReleaseNotes.pdf |
| Size: | 0.45 MB (476054 bytes) |
| MD5 Checksum: | 5cfb2b0c7c87c84d35acca8d54eeee08 |
| SHA512 Checksum: | c4eb836090a1867146d93d1ce74e490d... |

Security Advisory

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* |
|--------|----------|----------------|
| CSCwd59111 | "[BP-CUPS] [Syslogs] msid <310260390152986>, CSReq with HO received without valid fteid or with Remot" | cups-cp |
| CSCwc34754 | Active call got disconnected during handoff from 4G to wifi on ICSR setup with Gx-Alias enabled. | cups-cp |
| CSCwd66766 | cli display shows contradictory information for UP-Group name and UP-NODE-ID | cups-cp |
| CSCwd19379 | [BP-CUPS] call drops on sessmgr task kill - recover_sgx_from_crr failed | cups-cp |
| CSCwd99519 | [UPF-SVI] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce | cups-cp |
| CSCwe59693 | [CUPS] "show sx-serv stat" shows Discarded Prime PFD Management Response while all packets are ack | cups-cp |
| CSCwd27672 | [BP-CUPS]:Assertion failure at Function: sn_memblock_memcache_alloc() | cups-cp |
| CSCwe53561 | BP-CUPS : Sessmgr crash is observed after UP switchover when s8hr is configured on ICSR setup | cups-cp |
| CSCwe53128 | lpool-ip-validation-failed for overlap ip pool feature | cups-cp |
| CSCwe08636 | [BP-CUPS] Dynamic rule is not getting installed with no policy-control update-default-bearer | cups-cp |
| CSCvu76574 | [BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error | cups-up |
| CSCwd91525 | [CUPS-LI] Collisions were seen after UP planned and unplanned switchover in RCM setup | cups-up |
| CSCwe42821 | CUPS-UP] on Active UP SessMgr memory leak at sessmgr_uplane_allocate_uplane_clp_data | cups-up |
| CSCwc73243 | [BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721 | cups-up |
| CSCwe58228 | [CUPS UP] flow limit-across-applications non-tcp is not working in CUPS | cups-up |
| CSCwd72712 | [CUPS UP] gtpumgr shows memory warn in standby UP | cups-up |

| Bug ID | Headline | Product Found* |
|--------|----------|----------------|
| CSCwe42997 | [BP-CUPS] F132254 -warn state seen when applying 5000 ruledef's on Vodacom config | cups-up |
| CSCwe51492 | Sessmgr crash with function :: uplane_create_app_data_flow on Data UPs | cups-up |
| CSCwe17332 | IpsecDemux process restart due to invalid IpsecMgr id | epdg |
| CSCwc65963 | sessmgr restart is seen when configuring and unconfiguring Lawful intercept CLIs multiple times | mme |
| CSCwd29108 | [NSO-MOB-FP] error with nfv-vim package with NSO 5.7.6.2 or 5.8.4 or 5.6.8 and MFP 3.4 | nso-mob-fp |
| CSCwe45652 | PGW is not triggering UBR after RAR from PCRF for IP Filter Replace | pdn-gw |
| CSCwd75230 | AVP Framed-IP-Address missing in radius accounting when HO from LTE to VoWIFI | pdn-gw |
| CSCwd95524 | chkpointmgr pushing other active's info instead of failing active to the stby at SWO | rcm |
| CSCwd91543 | IKE notify packets are not responded after pod reload | rcm |
| CSCwd51484 | Apache Tomcat 9.0.0-M1 Req Smuggling and Azul Zulu java (2022-10-18) Mulitple Vulnerabilities | smi |
| CSCwd81548 | [5GaaS] Edge proxy NFs rely on NF restarts to apply config changes | smi |
| CSCwe51959 | v21.28.mx as the upstream branch :: RHEL-8 Build Issues fix in downstream Dev Branch v21.28.ZVx | staros |
| CSCwe55152 | SVI-P5G Rel 9.96.2: VPP restart along with core while deleting PODs - protocol-n0-1-0/1 | upf |
| CSCwe11650 | [UPF-SVI]-bulkstats process in warn state after overnight longevity | upf |
| CSCwd35335 | SFR: UPF not able to send trafic on E810 100Gbps links | upf |
| CSCwe29094 | [UPF-SVI] : Seen Uplane received invalid far id in PDU on task kill | upf |
| CSCwd60981 | [UPF] UPF does not initiate Sx_Session_Report_Req after receiving GTP_ERROR_IND_MSG | upf |
| CSCwe48926 | UPF is sending an additional link local address in next-hop for BGP UPDATE | 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* |
|--------|----------|----------------|
| CSCwc83349 | [sgw 140014 error] Failure dispatching event <SNX_MSGTYPE_SGW_ADD_PDN_REQ> during longevity test | cups-cp |
| CSCwd33517 | show apn statistics shows wrong value for GERAN and UTRAN users | cups-cp |
| CSCwd39954 | [CUPS-CP] Delay seen when CP handles 32 Sx associated UPs | cups-cp |

Resolved Bugs in this Release

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwe42876 | aaamgr in warn state for CP | cups-cp |
| CSCwc85511 | Disconnect reason for PureS call is different between CSL and CLI（Bulkstats) | cups-cp |
| CSCwe07449 | Crash Observed in 21.23.24 of CUPS CP | cups-cp |
| CSCwe17344 | [BP-CUPS] Fatal Signal 11: 11 PC: [0a2e24dc/X] check_n_update_gx_rules() | cups-cp |
| CSCwe54507 | Charging not happening for user moving from 4G to 5G | cups-cp |
| CSCwc95182 | SGW doesn't send DBR/DSR triggered by GTPU path failure | cups-cp |
| CSCwe01868 | SX collision in Delete IDFT and logs Misc Error3: Internal Failure : SX_MODIFY_REQ failed for Trans | cups-cp |
| CSCwe44005 | [BP-CUPS]21.28.3.88871:sessmgr crash has been seen after stopping the call model | cups-cp |
| CSCwc63031 | Sgsn change cdr prints wrong sgsn ip address when performing pureP to Collapsed Handover. | cups-cp |
| CSCwd87905 | [BP-CUPS] Observed sessmgr restart "free_acct()" during sessmgr kill in longevity setup. | cups-cp |
| CSCwe11497 | CDR written is coming as negative (-) value | cups-cp |
| CSCwe24070 | [BP-CUPS]: sessmgr crash at Function: acsmgr_collect_usage_for_all_monitoring_keys() | cups-cp |
| CSCwe06468 | CUPS CP: sessmgr restart seen in Function: sgwdrv_pdn_fsm_st_connected_evt_modify_bearer_ind() | cups-cp |
| CSCwd37844 | [BP-CUPS]Multiple occurrence sessmgr_nlp_gtpu_sess_abort_hndler()sessmgr_nlp_mqueue_timer_handler | cups-cp |
| CSCwd76879 | Sessmgr process restarted at function sessmgr_compress_call_info() | cups-cp |
| CSCwe46117 | [CUPS-CP] Error SX_MODIFY_REQ failed for Trans: Proc Type: SMGR_GGSN_MODIFY_REQ_QUERY_VOG | cups-cp |
| CSCwd66766 | cli display shows contradictory information for UP-Group name and UP-NODE-ID | cups-cp |
| CSCwe37928 | Observing sessmgr crash::sn_aaa_session_get_user_data | cups-cp |
| CSCwe41701 | [BP-CUPS]: Assertion failure at sess/snx/drivers/sgw/sgw_pdn_fsm.c:9958 | cups-cp |
| CSCwd96839 | CP triggers CCRU with RESOURCE_ALLOCATION_FAILURE performing 4gto3g Qos Change | cups-cp |
| CSCwd99900 | [CUPS] Traffic blocked when quota is preemtively request in addition to other RG redirected | cups-cp |
| CSCwe48599 | Sessmgr crash due to assertion failure in egtpc_handle_csfb_suspend_notf_evt function. | cups-cp |
| CSCwd93230 | "[CUPS UP] When dynamic rule precedence is zero, UP is not accounting packet in URR " | cups-up |
| CSCwc18750 | ARP Request have wrong Sender IP set to network address instead of interface address | cups-up |
| CSCwd96944 | Sessmgr instance restarted at function sessmgr_populate_pdr_in_teid_list() | cups-up |
| CSCwd46457 | SSD collection may cause BFD timeout with 16 vpp workers due to show memory main-heap | cups-up |
| CSCwd72712 | [CUPS UP] gtpumgr shows memory warn in standby UP | cups-up |
| CSCwe00049 | sessmgr memory usage is increasing while number of subscribers remains mostly the same | cups-up |
| CSCwd95901 | "CUPS UP - After sessmgr crash, sessmgr is not showing p2p as loaded in 'show module'" | cups-up |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwe14834 | [BP-CUPS]:sessmgr crash on UP " sessmgr_uplane_process_sx_update_far_update_tep_teid.part.1368()" | cups-up |
| CSCwe40695 | CUPS UP - ruledefs associated with host-pool are not working after UP Switchover | cups-up |
| CSCwe51492 | Sessmgr crash with function :: uplane_create_app_data_flow on Data UPs | cups-up |
| CSCwd94756 | Bulkstat counters show lower IPv6 throughput compared to real throughput | cups-up |
| CSCwe54365 | MME sets incorrect NRI container in ULR to VLR when receiving NRI container in attach-req | mme |
| CSCwe21358 | "KPI Counters / Bulk Stats for Extended QCI (65, 69) not available" | mme |
| CSCwd71339 | Increase in DUCON_NSA errors / path switch failures | mme |
| CSCwe40765 | [MME] GNodeB Lookup fails for the connected gnb received in config update message | mme |
| CSCwe56368 | Sessmgr crash due to assertion failure in sn_gt_handle_mm_req_failure function. | mme |
| CSCwc95044 | MME continues to use blockedlisted SGW | mme |
| CSCwd68562 | ASR5500 - MME- 21.25.4 (83215) - MMES1PathFail increase | mme |
| CSCwb72536 | Display of IP address is not proper with dual stack enabled in s1-mme | mme |
| CSCwd97399 | Observing mmemgr crash:: cmPAsnDecChExt | mme |
| CSCwe30923 | Observing sessmgr crash with function :: egtpc_resume_suspended_proc() | mme |
| CSCwd73793 | Assertion failure at sess/mme/mme-app/app/mme_pdn_fsm.c:829 | mme |
| CSCwe54464 | Multiple mmemgr and sessmgr restart observed in eMBMSsuite | mme |
| CSCwd52626 | Assert at egtpc_resume_suspended_proc() | mme |
| CSCwc53423 | Sessmgr task restart on sess/egtp/egtpc/egtpc_evt_handler_func | pdn-gw |
| CSCwd40511 | sessmgr restart on acsmgr_process_tcp_packet | pdn-gw |
| CSCwd67200 | Incomplete MSISDN in servedMSISDN CDR field | pdn-gw |
| CSCwd80515 | PGW not binding Gx Dynamic rule for dedicated bearer in WiFi to LTE handoff scenario | pdn-gw |
| CSCwe23018 | CLI corruption in the output after running "update active-charging override-control rulebase-config | pdn-gw |
| CSCwd02729 | Continuous EGTPCPathFailClear traps after receiving echo requests during no session | pdn-gw |
| CSCwd46286 | "Gy Server returns RC 5030 causing Assume Positive to kick in, CCR-T will contain USU with all zero" | pdn-gw |
| CSCwd55724 | Duplicate Precedence assignment by PGW in TFT packet Filters | pdn-gw |
| CSCwd65441 | E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query | pdn-gw |
| CSCwc83287 | [Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression | pdn-gw |
| CSCwc88534 | Diagnostic code for unexpected dra peer switch | pdn-gw |
| CSCwd30312 | MPLS LDP neighbors no existing after SPGW SW upgrade | pdn-gw |

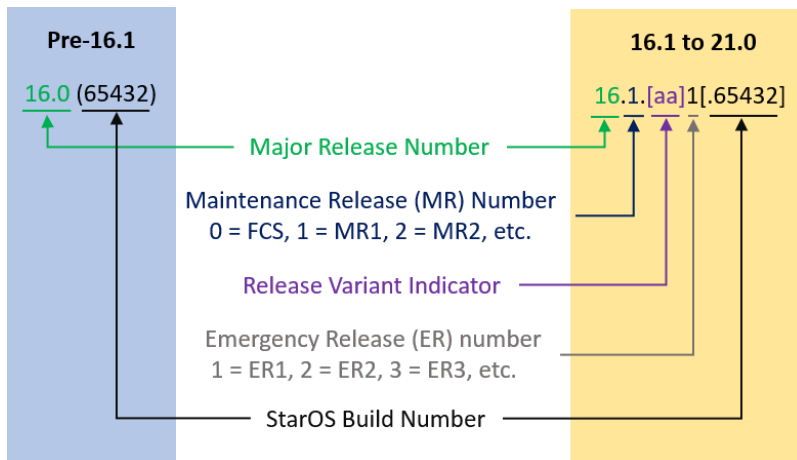| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwd32146 | ?Update Bearer Request? is send PGW->SGW without EPS Bearer QoS, which is not aligned with 3GPP | pdn-gw |
| CSCwd39197 | E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query | pdn-gw |
| CSCwe15218 | Diamproxy Restart After FQDN Configuration on Gy Endpoint | pdn-gw |
| CSCwe21674 | Authentication Failing during UDP Socket Creation when using IP VRF Forwarding | pdn-gw |
| CSCwa49391 | [BP-CUPS] Traffic Optimization UP stats not getting incremented/decremented properly | pdn-gw |
| CSCwc09456 | Sessmgr instance restart due to assertion failure at acs/acsmgr/acsmgr | pdn-gw |
| CSCwc97269 | APN configuration getting removed | 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 |
| CSCwd44164 | sessmgr task unexpected restarted occurred on PGW acs_http_accel_check | pdn-gw |
| CSCwd79989 | checkpoint manager statistics are broken | rcm |
| CSCwd64943 | [SAEGW] - ASR5500- - 21.23. 12 ICSR Standby sessmgr in Memory over state | sae-gw |
| CSCwd99902 | Assertion Failures triggered during ADMF provisioning/auditing LI configuration | sae-gw |
| CSCwe24837 | New sessions accepted while APN set with newcall policy reject | sae-gw |
| CSCwd75398 | PDP for some 2G (only) capable UE s are getting disconnected with cause - sgsn-isr-addl-ptmsi-rai | sgsn |
| CSCwe04086 | Sessmgr Restart at sess/sgsn/stackmgr/sn_gprs_gtp.c | sgsn |
| CSCwd41111 | [S8HR] SGW increments "Apn Lookup Failed" wrongly for packets sent over non-s8hr bearers | sgw |
| CSCwc69565 | [S8HR] show lawful-intercept s8hr statistics all display the wrong ebi value | sgw |
| CSCwd41016 | No session deletion after S5 path failure followed by bearer resource command | sgw |
| CSCwe00358 | Mbreq over Mbreq drop show config error log | sgw |
| CSCwe36928 | [ares] AFIO - by default disable fabric device register dump collection when DCH FIFOs overflow | staros |
| CSCwd65439 | Password change option for user in warning period before expiration. | staros |
| CSCwd60503 | Hermes - Provide the fix for critical issues reported on StarOS. | staros |
| CSCwd80626 | Placeholder for fixing third party libraries related issues in StarOS - Hermes | staros |
| CSCwd74056 | [UPF] IPv4v6 PDN Data Statistics not updated correctly for packet drops due to flow discard | upf |
| CSCwe30498 | "[UPF]Time quota is not reset post UPF 1:1 ICSR, in case new quota is not provisioned." | upf |
| CSCwe10556 | [UPF] Flow Idle timing out even thought traffic is seen on fastpath | upf |
| CSCwd56118 | [UPF]Data throttled at inaccurate rate for certain bit rates above 4.2 G | upf |
| CSCwe11674 | [SVI-cnUPF]: ipsecctrl is in warn state after 12hrs run | upf |
| CSCwd94275 | [SVI-UPF]: After upf reloads "vpp_main" still stays in warn state | 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.
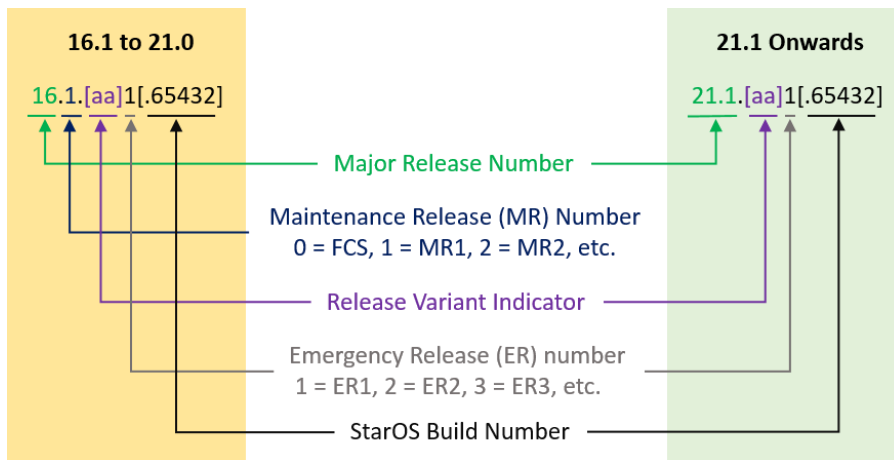
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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".

Pre-16.1

16.0 (65432)

16.1 to 21.0

16.1.[aa]1[.65432]

Major Release Number

Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.

Release Variant Indicator

Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.

StarOS Build Number

The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, "21.1.1".

16.1 to 21.0

16.1.[aa]1[.65432]

21.1 Onwards

21.1.[aa]1[.65432]

Major Release Number

Maintenance Release (MR) Number
0 = FCS, 1 = MR1, 2 = MR2, etc.

Release Variant Indicator

Emergency Release (ER) number
1 = ER1, 2 = ER2, 3 = ER3, etc.

StarOS Build Number

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)