Release Notes for StarOS™ Software Version 21.22.13

First Published: May 6, 2022
Last Updated: May 6, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.22.8. 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	21.22.13, build 85011

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.

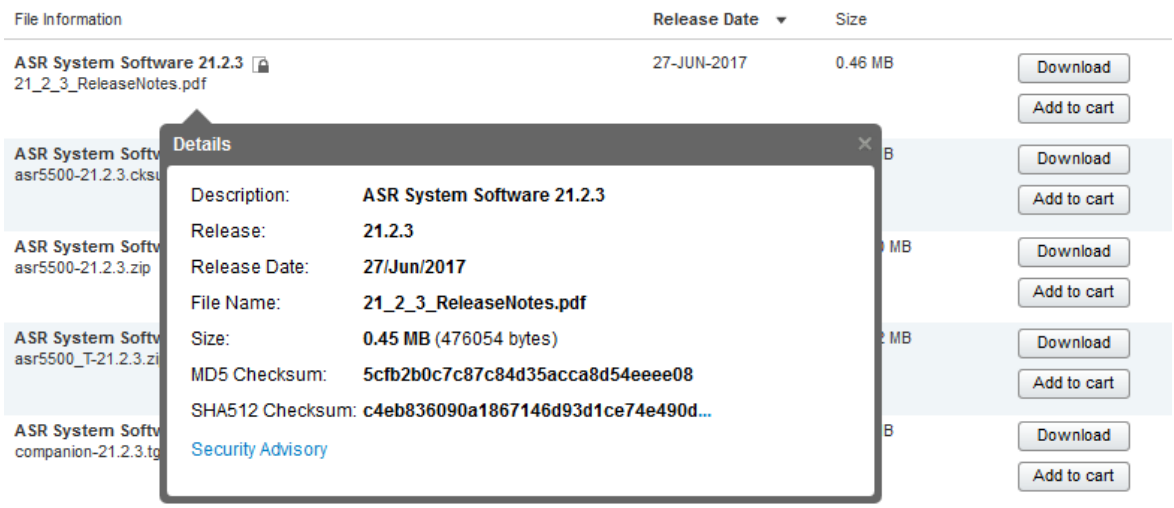
Firmware Updates

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 > certutil.exe -hashfile *<filename>.<extension>* SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 *<filename>.<extension>*

Linux	Open a terminal window and type the following command
	
	$ sha512sum *<filename>.<extension>*
	
	Or
	
	$ shasum -a 512 *<filename>.<extension>*

NOTES: *<filename>* is the name of the file. *<extension>* is the file extension (e.g. .zip or .tgz).	

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

Certificate Validation

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

Open Bugs in this Release

The following table lists the known bugs that were found in, and remain open in this software release.

NOTE: This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the Cisco Bug Search Tool.

Table 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvx29537	[BP-CUPS]acsmgr_create_cr_defn()process_install_requests()acs_process_received_policy()	cups-cp
CSCvv13409	[BP-CUPS]URR node not found at CP for URR-id: 0x82 received in Usage Report	cups-cp
CSCvw83826	[BP-CUPS]: Huge session disconnect with reason "sxfail-opr-remove-pdr"	cups-cp
CSCvx33850	Rulename associated with PDR is not displayed in "show cli" output	cups-cp
CSCwa29010	[BP-CUPS] "show config error" does not show errors.	cups-cp
CSCvv14996	[BP_CUPS] Timedef rule matches if no timedef is configured	cups-up
CSCwa18164	Counter rolls over frequently due to inappropriate data-type (e.g. sgw-datastat-dl-qci8totbyte)	cups-up
CSCvy57500	[BP-PCT] Incorrect bytes and pkts seen for http analyzer stats.	cups-up
CSCvz41620	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync	cups-up
CSCwa75811	For 3G to 4g TAU for DECOR subscriber MME is introducing 10s delay for SGSN context request message	mme
CSCvy61494	multi fault with sessmgr restart Function: mme_app_fill_s1_bearer_values()	mme
CSCvy02339	Parameters are encoded wrongly at MME and sent to GMPC server	mme
CSCvu37233	Multiple Sessmgr restarts seen while doing service card migration from active to standby	mme
CSCvx66296	Assertion failure at mme_app_destroy_ue_sgw_pdn_ctxt()	mme
CSCvx53094	sessmgr restart seen in function mme_app_fill_s1_bearer_values()	mme
CSCvw25217	BP-ICUPS : sessctrl crashes during boot up at acs_sanitize_a_single_tdb	pdn-gw
CSCvw58020	Non WPS session : PGW not responding to MBReq - SRVCC without PS handover	sae-gw
CSCvy33792	[VPC-DI] SAMOG Increase cisco-mpc-protocol-interface AVP length for eogre_pmipv6	samog

Bug ID	Headline	Product Found*
CSCvy02352	Parameters are encoded wrongly at SGSN and sent to GMPC server	sgsn
CSCvy09744	[CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt	sgsn
CSCvz64429	Failed to load MIB modules from starent.my error	staros
CSCwa12029	MIOs Cards is crashing due to bad minicores	staros
CSCvy77792	vpnmgr restart seen @ sn_slist_lookup_by_key()	staros
CSCvz46069	IPv6 Mgmt IP not reachable after CF switchover	staros
CSCvz80896	[UPF]: Next-hop row is not created if next-hop cli is added in middle of the call	upf
CSCvw74614	[Combo-UPF]: Peer ID is not displayed correctly in show sx peers cli	upf
CSCwa75370	[Combo-UPF] Uplink data is not getting offloaded after Converged to Non-Converged SGW Relocation	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*
CSCvy66595	CP does not create the Redirect-FAR for FUI-redirect	cups-cp
CSCwa05413	CUPS CP - GGSN-C - Unexpected UPC request after HO to 3G of 2 PDN's to the same APN	cups-cp
CSCwb02662	[CUPS CP] sessmgr restart is seen in Function: sn_aaa_session_set_user_data()	cups-cp
CSCvs48614	[BP-CUPS] bulk of ipsec 56745 error logs seen during up icsr with single call	cups-cp
CSCwa37853	Multiple sessmgr crashes and traffic drop after making active-charging service changes on CP.	cups-cp
CSCvy63380	CUPS CP Adds Null Value 0.0.0.0 as the servingNodeAddress in PGW-CDR (PERMANENT FIX)	cups-cp
CSCvy79949	CUPS IDFT SGWCDR RecClosingCause	cups-cp
CSCvz97998	"[CUPS CP] causeForRecClosing set to "Management Intervention" for session with rulebase-list,"	cups-cp
CSCvy56389	After SR only one CCR-U sent due to Validity Timer expiry and VT stopped even though MSCC is active.	cups-cp
CSCvz09324	URR node not found at CP for URR-id: 0x80000009	cups-cp
CSCwa61799	[CUPS] 4G->2G/3G->4G HO failures - double traffic endpoint deletion	cups-cp
CSCwa33471	Sess mgr restart: Assertion failure at pgw_interface Function: pgw_drv_handle_events_from_smgr	cups-cp
CSCwb03324	CUPS CP - Unexpected UPC request from CUPS GGSN after QOS change in 3G occurs	cups-cp
CSCvy94185	Tariff Time Change CDR Issues | Support for Tariff Time Switch through Gy AVP “Tariff-Time-Change	cups-cp
CSCvz94587	One way traffic broken in CUPS with 4Gto2g(CSFB)to3Gto4G handover	cups-cp
CSCwa00750	UP allows packets and reports usage even when under FUI-Terminate	cups-cp
CSCwa56879	Fatal 11 at sessmgr_sgw_send_sx_modify_req_trgr_mbreq_init_attach	cups-cp
CSCwa75114	Cache not cleared when association of all UPs	cups-cp
CSCwb06211	CUPS CP :counter SAEGW.pgw-sesstat-pdn-rat-geran is never reset on 21.23	cups-cp
CSCwa53617	[CUPS CP] CP is not sending Update QER during 3G UPC (HLR initiated Qos change)	cups-cp
CSCwb23375	"CP sends SX PFD messages, despite 'sx-pfd-push disabled' being configured under the user-plane-group"	cups-cp
CSCwa33658	sessmgr 12325 error "Uplane received invalid far id in PDU"	cups-cp
CSCwa56054	Complete Fix for Monitoring time chekpointing Issues	cups-cp

Bug ID	Headline	Product Found*
CSCvz92880	vpp thread/memif mapping issue after (double) sessmgr restart	cups-up
CSCwa83817	[CUPS-UP] Some UP does not activate VPP correctly after upgrade or reload	cups-up
CSCwa87288	SIP invite not initiated from UPF to UE	cups-up
CSCvz50778	CUPS UP - Packets stuck in VPP queue under unknown conditions	cups-up
CSCwb01365	[CUPS-UP] SessMgr task restart while generating partial CDR due to secRat reports	cups-up
CSCwb27606	[CUPS-UP]Crash at sx_tun_fsm_handle_sess_mod_rsp_evt	cups-up
CSCwa92158	[BP-CUSP] TCP Accelerator relative sequence number calculation following 2^32 wrap round	pdn-gw
CSCvx82177	sessmgr restart "sessmgr_tcp_conn_close_v6_v4()"	pdn-gw
CSCwa81196	Externally exposed HTTP ports on RCM	rcm
CSCvy00182	Cisco RCM for StarOS Software TCP Denial of Service Vulnerability	rcm
CSCwb19420	[PLT-RCM] RCM apply_config script giving errors	rcm
CSCvy79548	bfdmgr does not send keepalive - Intermittent	rcm
CSCwb42558	Upgrade Spring Framework to version 5.2.20	rcm
CSCwa37651	SGW CDR not containing all RANSecondaryRATUsageReport - underbilling	sgw
CSCvz28910	Supporting 25G link speed in staros linux kernel code for drivers(i40evf)	staros
CSCwa73707	ssh server config 'client-alive-countmax' is not working	staros
CSCwa94328	[BP -CUPS] Sx down after SF reboot followed by CF switchover	staros
CSCwa29851	"After SessMgr Recovery, session manger is not sending sx-peer-node info to RCM/Standby Chassis"	upf
CSCwa92472	Packet drop at sessmgr after atomic frag header removal	upf
***** Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

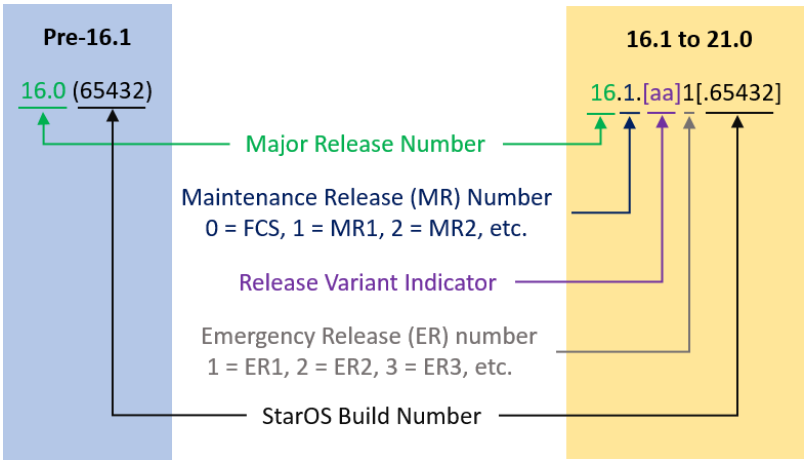
StarOS Version Numbering System

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

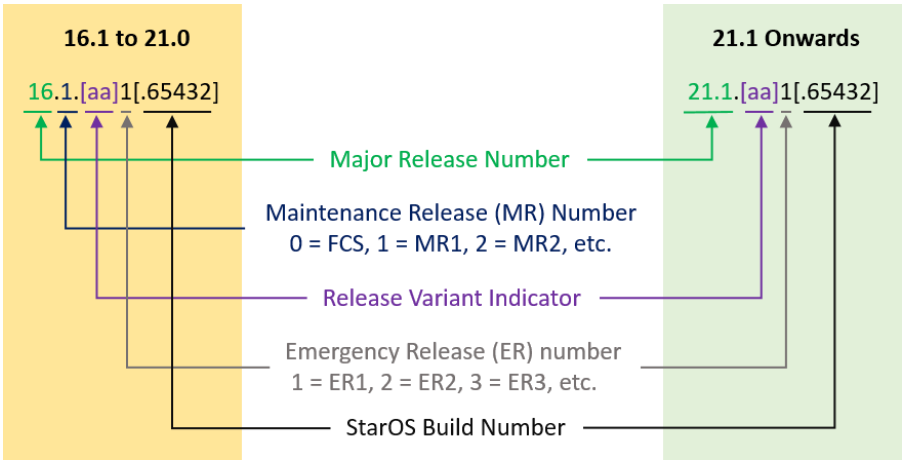
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example “16.1.2”.



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



In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

Release Package Descriptions

Table 5 provides descriptions for the packages that are available with this release.

Table 5 - 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. In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC-DI		
qvpc-di-<release>.bin.zip	qvpc-di-<release>.bin	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.bin.zip	qvpc-di_T-<release>.bin	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di-<release>.iso.zip	qvpc-di-<release>.iso	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-di_T-<release>.iso.zip	qvpc-di_T-<release>.iso	Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

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

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. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.iso.zip	qvpc-si_T-<release>.iso	Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware-<release>.zip	qvpc-si-template-vmware-<release>.ova	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-vmware_T-<release>.zip	qvpc-si-template-vmware_T-<release>.ova	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm-<release>.zip	qvpc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-template-libvirt-kvm_T-<release>.zip	qvpc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si-<release>.qcow2.zip	qvpc-si-<release>.qcow2.gz	Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
qvpc-si_T-<release>.qcow2.zip	qvpc-si_T-<release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.

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. In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 6 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 6 - 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.