



Release Notes for StarOS™ Software Version 21.28.m0

First Published: December 22, 2022

Last Updated: December 22, 2022

Introduction

This Release Note identifies changes and issues related to this software release. This major release is based on release 21.28.0. These release notes are applicable to StarOS PGW, SAE-GW & ICUPS products.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.28.m0, build 88143

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 the complete list of CUPS documentation available for this release, go to <https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html>.

For the complete list of the corresponding StarOS documentation, go to <https://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.

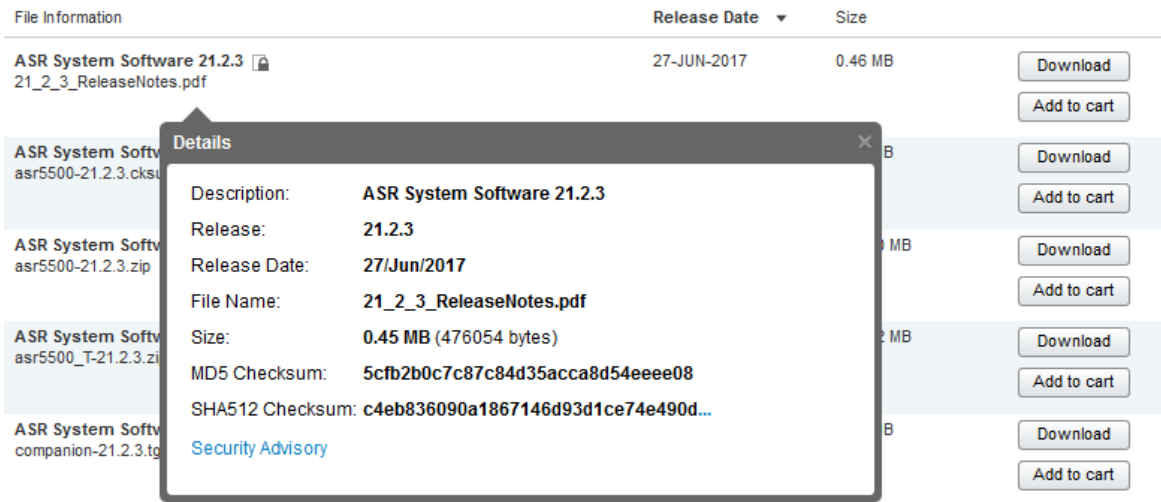
Firmware Updates

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

Open Bugs in this Release

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*
CSCwd93297	[BP-CUPS] Observed smgr restart "egtpc_handle_create_sess_req_msg_at_pgw_ingress" in E fence build	cups-cp
CSCwd94049	[BP-CUPS]observed smgr restart "acsmgr_check_n_delete_pdrs_for_deleting_bearer" in E fence build	cups-cp
CSCvu48856	[BP-CUPS]: [gtpc 47514 error] GTPC Misc error: Deactivation already in progress.	cups-cp
CSCwc41191	[BP-CUPS][sessmgr 12341 error]<sessmgr:19> sessmgr_uplane.c:36963][SXB]Updated URR doesn't exist.0x27	cups-cp
CSCwd27672	[BP-CUPS]:Assertion failure at Function: sn_memblock_memcache_alloc()	cups-cp
CSCwd87905	[BP-CUPS] Observed sessmgr restart "free_acct()" during sessmgr kill in longevity setup.	cups-cp
CSCwd59111	"[BP-CUPS] [Syslogs] msid <310260390152986>; CSReq with HO received without valid fteid or with Remot"	cups-cp
CSCwd42172	[BP-CUPS] ECS matches TCP ACK with non-zero length segment to ruledef with tcp payload-length = 0	cups-up
CSCwd84011	[CUPS] eDNS enrichment is not working	cups-up
CSCwd88991	[CUPS-UP]: Packets stats not coming correct after quota exhaustion for TCP v4 traffic	cups-up
CSCwd90855	[BP-CUPS] Observed stats issue while validating the analyzer statistics for TCP	cups-up
CSCwc73243	[BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721	cups-up
CSCwd80215	[BP-CUPS] Observed "sx-mand-ie-incorrect" disconnects post PFD push complete	cups-up

Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwd83922	[CUPS-UP]: Incorrect values under cli "show up-event-record statistics interface-type sxb";	cups-up
CSCwd91525	[CUPS-LI] Collisions were seen after UP planned and unplanned switchover in RCM setup	cups-up
CSCwd94756	Bulkstat counters show lower IPv6 throughput compared to real throughput	cups-up
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
CSCwd75230	AVP Framed-IP-Address missing in radius accounting when HO from LTE to VoWIFI	pdn-gw
CSCwd91543	IKE notify packets are not responded after pod reload	rcm
* 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*
CSCwc97463	session manager restart and crashes occurs after triggering the call model	cups-cp
CSCwc07775	Unable to configure ECSv2 limits of scale after CF switchover	cups-cp
CSCwd37844	[BP-CUPS]Multiple occurrence sessmgr_nlp_gtpu_sess_abort_hdlr()sessmgr_nlp_mqueue_timer_handler	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwc19599	Gy credit control failure handling not working when Gy link is down between CP and OCS	cups-cp
CSCwb52197	"[CUPS UP] VPP/hatsystem restart cli_b_memcpy_fast() during IP routes consolidation in BGP, "	cups-up
CSCwb96703	[CUPS 21.27.2.85330] UP Session manager crash when charging-action is missing in config	cups-up
CSCwb75761	Multiple session manager restart - sessmgr_process_init_config	cups-up
CSCwb40992	[BP_PCT] Delete IPs from readdress server list is not working in 21.27.G0.xxxx	cups-up
CSCwb55459	[BP-CUPS]:Assertion failure at sctrl_cfg_sync_decode_traffic_optimization_profile_config_tlv()	cups-up
CSCwc96489	[BP-CUPS] Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23721	cups-up
CSCwc82316	"Recovery after Gy bypass (SU for CCR-I/CCR-U), UP drops all subscriber packets"	cups-up
CSCwb37060	5G statistics attempt/success/failure increments when License is not enabled	epdg

Operator Notes

Bug ID	Headline	Product Found*
CSCwc08120	Incorrect Message Level [ipsec 55609 critical] [4/0/10468 <ipsecmgr:284>ipsecmgr_msg.c:1449]	epdg
CSCwd10265	[5GaaS] MME sending wrong destination realm resulting in 3002 from DRA	mme
CSCwc80299	"CBC , MME send Write Replace Warning Indication before Write Replace Warning Response"	mme
CSCwb53675	[MME] release-due-to-pre-emption (39) S1AP radio network cause not implemented	mme
CSCwd68562	ASR5500 - MME- 21.25.4 (83215) - MMES1PathFail increase	mme
CSCwb90376	MMEs is generating 00 values on the bulkstat for one of the VLRs	mme
CSCwa92047	MME: Authentication info to UE not sent during TAU when decor enabled.	mme
CSCwc93870	DCNR Devices and Attached DCNR calls shows different values	mme
CSCwd08401	MME requirement in the 3GPP Specifications with respect to EPS to 5GS Mobility registration	mme
CSCwc59471	sessmgr in warn/over state due to mme_app_allocate_s1nas_msg and SN_cmAlloc()	mme
CSCwc99355	Target MME sending Source SGW IPv6 address in Handover Request	mme
CSCwd93433	Sessmgr crash at mme_app_check_and_mark_pra()	mme
CSCwa52782	Node reloaded after LAG group port reconfiguration	pdn-gw
CSCwb81718	CCR-U/CCR-T for Non-WPS session going through WPS channel	pdn-gw
CSCvy78942	With WPS3B configuration GW use secondary PAS during mid-session	sae-gw
CSCwb58656	sessmgr restart due to Assertion failure at sess/smgr/sessmgr_hlcom.c:467	sae-gw
CSCwb65556	Observing sessmgr crash:: sessmgr_get_num_mnc_digits	samog
CSCwb79049	Handover :Frozen sessions seen in SGSN after 2g-4g handover	sgsn
CSCwd17474	Trusted build: StarOS password encryption improvement feature new format saving issue	staros
CSCwb41992	MACs algorithm configuration does not operate as expected	staros
CSCwd17799	[UPF-SVI] : Client-ID : n/a in sho sub user-plane-only callid 042cf7f5 flows full	upf
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

StarOS Version Numbering System

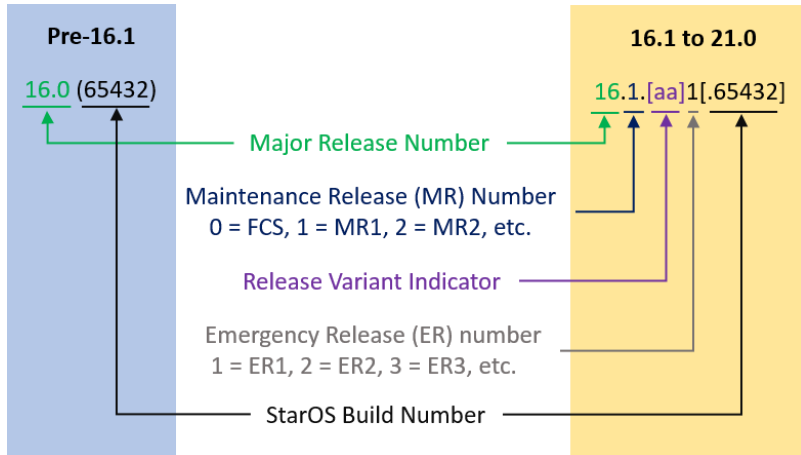
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

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.

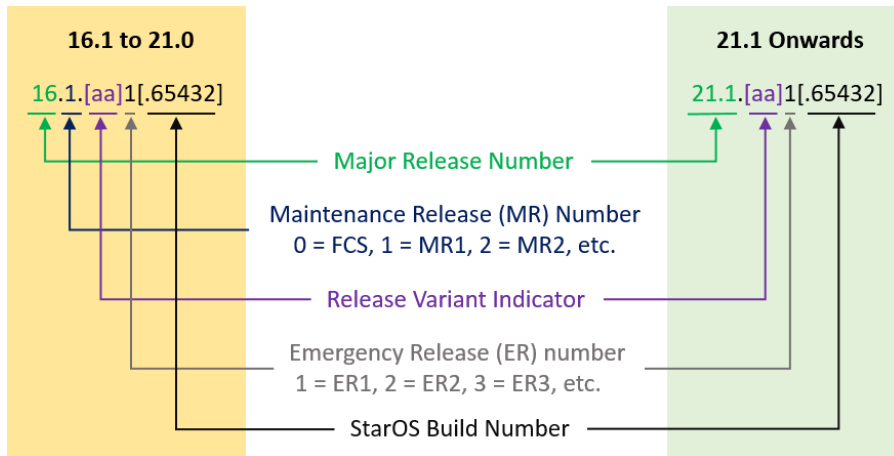
Operator Notes

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 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		
qvp-di-<release>.bin.zip	qvp-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.
qvp-di_T-<release>.bin.zip	qvp-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.
qvp-di-<release>.iso.zip	qvp-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.
qvp-di_T-<release>.iso.zip	qvp-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
qvmc-di-template-vmware-<release>.zip	qvmc-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>
qvmc-di-template-vmware_T-<release>.zip	qvmc-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>
qvmc-di-template-libvirt-kvm-<release>.zip	qvmc-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>
qvmc-di-template-libvirt-kvm_T-<release>.zip	qvmc-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>
qvmc-di-<release>.qcow2.zip	qvmc-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>
qvmc-di_T-<release>.qcow2.zip	qvmc-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>
VPC-SI		
qvmc-si-<release>.bin.zip	qvmc-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>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-si_T-<release>.bin.zip	qvmc-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>
qvmc-si-<release>.iso.zip	qvmc-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>
qvmc-si_T-<release>.iso.zip	qvmc-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>
qvmc-si-template-vmware-<release>.zip	qvmc-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>
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>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qnpc-si_T- <release>.qcow2.zip	qnpc-si_T- <release>.qcow2.gz	Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.
VPC Companion Package		
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.

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)

© 2022 Cisco Systems, Inc. All rights reserved.