Release Notes for StarOS™ Software Version 21.25.15

First Published: April 13, 2023
Last Updated: April 13, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.25.14. These release notes are applicable to the ASR5500, VPC-SI ,VPC-DI and RCM platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.25.15, build 89364

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 > 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*
CSCvz44140	[BP-CPUS] mostly all aaamgr goes in warn state while running call model	cups-cp
CSCwd40162	[BP-CUPS] sesmgr crash: Assertion failure at sess/smgr/sessmgr_fsm_func.c:10998	cups-cp
CSCwc42330	Observed Sessmgr crash on CP:: "sessmgr_pgw_handle_create_bearer_cfm"	cups-cp
CSCwe91366	"URR node not found at CP for URR-id" of URR-id ended with 1 or 2	cups-cp
CSCwa08379	APN without IP pool name not able to serve call despite having free IPs.	cups-cp
CSCwa54600	[BP-CUPS] Assertion failure @ PC: [08dc3801/X] fill_dyn_chrg_rule_name_info()	cups-cp
CSCwd10514	CUPS 'clear subscribers' documentation updates	cups-cp
CSCwd14939	[CUPS-CP] Incorrect duration for time limit triggered CDRs after configuration change	cups-cp
CSCwd34520	CUPS (21.25.10) Assertion failure at sess/smgr/sessmgr_pgw.c:21482	cups-cp
CSCwd40067	4G QOS sent on UP after CCA-U while UE still in 3G	cups-cp
CSCwd55835	Pure-P to Collapsed and Collapsed to Pure-P Handovers are supported in CUPS	cups-cp
CSCwe30123	VPC - [SAEGW] - 21.25.10 (86143) - High level of service denied on SAEGW	cups-cp
CSCwd19554	[BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot	cups-cp
CSCwd19632	Assertion failure at sessmgr_app_svr_event_control_dispatch	cups-cp
CSCwd60353	CUPS - SAEGW - 21.25.10 - acsmgr_process_qgr_and_create_pdr_far	cups-cp
CSCwe61003	[CUPS-CP] Unexpected "URR node not found at CP for URR-id" logs observed	cups-cp
CSCwc07644	[BP-CUPS]AF at sess/smgr/sessmgr_gr_sess.c:1368 sessmgr_gr_handle_session_full_checkpoint on standby	cups-cp
CSCvz73626	sessmgr assert @ smgr_uplane_config_rule_options()	cups-up

Bug ID	Headline	Product Found*
CSCwa92931	[CUPS-LI-TLS] X3 index for heartbeat is not removed after removing LI config	cups-up
CSCvz49026	[BP-CUPS] sessmgr restart @ sn_memblock_memcache_alloc()	cups-up
CSCwe62837	difference between CUPS and ASR5500 in case of redirected flow getting reclassified	cups-up
CSCwb75761	Multiple session manager restart - sessmgr_process_init_config	cups-up
CSCwb55459	[BP-CUPS]:Assertion failure at sctrl_cfg_sync_decode_traffic_optimization_profile_config_tlv()	cups-up
CSCwb16852	"F102857 : ECS config corrupted on UP, after removing Sx-Association or removing ECS config on CP"	cups-up
CSCwe70286	"ePDG PLMN handoff attempts,success counters having same values in CLI"	epdg
CSCwd68562	ASR5500 - MME- 21.25.4 (83215) - MMES1PathFail increase	mme
CSCwd38978	MME is not responding to default IMS PDN Connectivity message	mme
CSCwe51260	mmemgr crash	mme
CSCwe21358	"KPI Counters / Bulk Stats for Extended QCI (65, 69) not available"	mme
CSCwc95044	MME continues to use blockedlisted SGW	mme
CSCvz46024	[CP-MME] sessmgr restart at egtpc_handle_mod_bearer_cmd_req_evt	mme
CSCwd52626	Assert at egtpc_resume_suspended_proc()	mme
CSCwd38108	Documentation: cli after-attach information not included in user guide	mme
CSCwd71339	Increase in DUCON_NSA errors / path switch failures	mme
CSCwb69510	The assert is hitting when mme handles the context response with failure cause code from the peer	mme
CSCwb59168	Encoding error @Stop-Warning-Indication message for multiple eNB-ID in "Broadcast-Empty-Area-List"	mme
CSCwc60621	MME: Assertion failure at sess/mme/mme-app/app/mme_app_egtpc.c:10901	mme
CSCwc68983	MME Sending incorrect TAC to SGW on Delete Session Request messages	mme
CSCwd17450	DDN option available under network-overload-protection cli not showing TEID-0 info	mme
CSCwc82786	MME Sending twice ULR as part of 5g-4g HO Followed by TAU	mme
CSCwd40838	mme sessmgr restart at mme_app_do_sgw_dns_query	mme
CSCwd91474	New calls are accepted even new call policy is configured as reject	mme
CSCwa50873	Many session disconnect reasons are not documented	pdn-gw
CSCvz76252	[BP-ICUPS] buffer leak found at VPP with regular callmodel sessions on the chassis	pdn-gw
CSCwa11844	BP-ICUPS: aaamgrs are going to over state due to high memory usage	pdn-gw
CSCwa41502	BP-ICUPS: sessmgr segmenattaion fault at sn_msg_arriving_handle()	pdn-gw

Bug ID	Headline	Product Found*
CSCvy90872	"BP-ICUPS: VPP restart while running the callmodel, resulted in segmentation fault"	pdn-gw
CSCwa54994	BP-ICUPS: sm reload at sn_memblock_cache_block_flush.part.1()	pdn-gw
CSCwc97269	APN configuration getting removed	pdn-gw
CSCwe71916	Sessmgr crash due to assertion failure in pgw_drv_fill_bearer_info_from_egtpc function.	pdn-gw
CSCvz70919	RCM OVF deployment for 21.25.x image is not succeeding	rcm
CSCwc26449	[PLT-RCM] Ubuntu 18.04 LTS / 20.04 LTS / 21.10 / 22.04 LTS : OpenSSL vulnerability (USN-5488-1)	rcm
CSCwa49484	RCM workaround for unreliable alert-forwarder	rcm
CSCvz61597	[SGIR-Ph1] After first switchover some profiles are in unknown state initially in save & reload case	sae-gw
CSCvz65453	[SGIR-Ph1] After MIO switchover sgi-reachability profiles status showing as DOWN	sae-gw
CSCwb65556	Observing sessmgr crash:: sessmgr_get_num_mnc_digits	samog
CSCvz94977	Maximum number of NTP servers	staros
CSCvy50485	[SVI-UPF]: vpp restarts at sn_assert_signal_handler()	upf
CSCvz47574	[UPF SVI] :- PCF initiated Dedicated bearer creation is not working [EPSFB] on hSMF	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*
For Resolved Bugs please contact CISCO customer support team.		
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

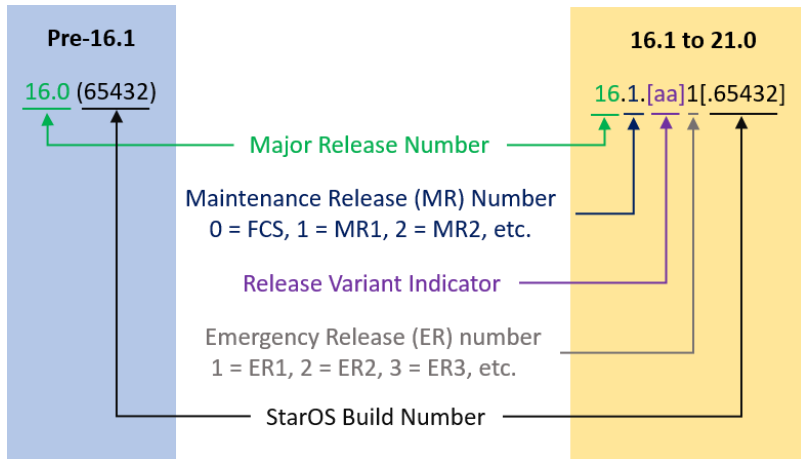# Operator Notes

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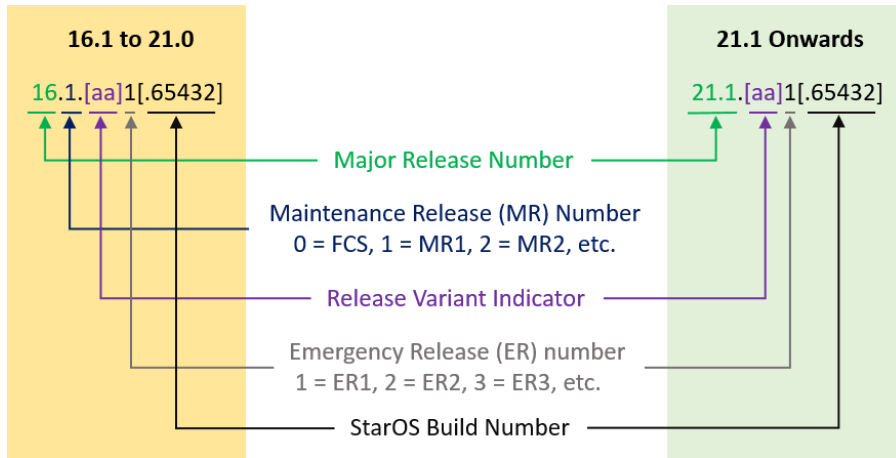
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

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 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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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.
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.