# Release Notes for StarOS™ Software Version 21.27.6

**First Published:** March 16, 2023
**Last Updated:** March 16, 2023

## Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.27.5. These release notes are applicable to the ASR5500, VPC-SI ,VPC-DI platforms and RCM platform.

## Release Package Version Information

**Table 1 - Release Package Version Information**

| Software Packages | Version |
|---|---|
| StarOS packages | 21.27.6, build 89241 |

## Feature and Behavior Changes

For information on feature and behavior changes associated with this release, refer to the *CUPS Release Change Reference*, and the corresponding *StarOS Release Change Reference*.

## 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.

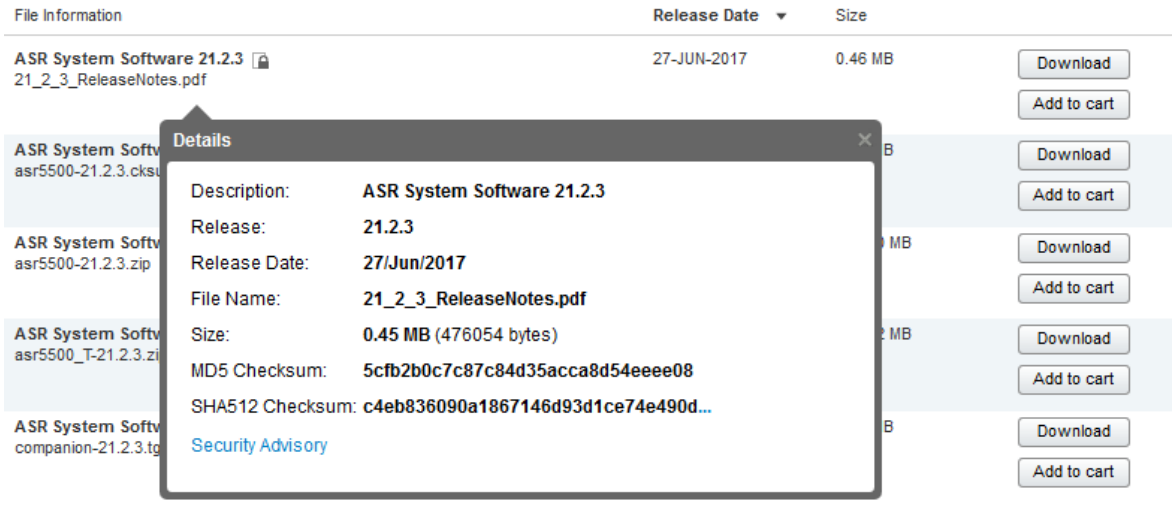
## Firmware Updates

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<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* |
|---|---|---|
| CSCwa83375 | [BP-CUPS] Observed sessmgr restart : snx_sgw_driver_handle_modify_rsp on CP in Longevity setup | cups-cp |
| CSCwc34754 | Active call got disconnected during handoff from 4G to wifi on ICSR setup with Gx-Alias enabled. | cups-cp |
| CSCwd19379 | [BP-CUPS] call drops on sessmgr task kill - recover_sgx_from_crr failed | cups-cp |
| CSCwd19554 | [BP-CUPS] memory bloating at acsmgr_cups_allocate_charging_snapshot | cups-cp |
| CSCwc12852 | [CUPS-BP] Admin Guide - Servers Unreachable - Specify non-support for after-timer-expiry | cups-cp |
| CSCwc81923 | CUPS LI Admin guide needs to remove SaMOG and ePDG related support | cups-cp |
| CSCwd09301 | RMMGR in Warn State on all Active SFs of CUPS-CP | cups-cp |
| CSCvu76574 | [BP-CUPS] recovery-invalid-crr-clp-uplane-gtpu-session checkpoint error | cups-up |
| CSCwb83398 | [BP-CUPS]Lots of error logs GTPU Recover Session Failed for GTP-u Peer on standby UP | cups-up |
| CSCwc82316 | "Recovery after Gy bypass (SU for CCR-I/CCR-U), UP drops all subscriber packets" | cups-up |
| CSCwc97902 | [BP-CUPS] V6 peers not coming up due to cause PFCP_CAUSE_REQUEST_REJECTED | cups-up |
| CSCwc53344 | [BP-CUPS] Function:  Assertion failure sessmgr_func.c:37116 Function: sessmgr_get_session_entry | cups-up |
| CSCvz03179 | [BP-CUPS] Assertion failure @ func sessmgr_uplane_check_calls_on_rulebases | cups-up |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwc95490 | Assertion failure at sess/sctrl/sessctrl_rcm.c:326-Func-sctrl_config_rcm_service() | cups-up |
| CSCwe60630 | CLI task restart during SSD collection | mme |
| CSCwe28302 | PLR with only IMEI option is not working | mme |
| CSCwd19318 | Enabling masked-imeisv only working for one mme-service when there are 2 mme-service | mme |
| CSCwc95163 | "[NSO-MOB-FP] p2p plugin has since release 2.65, 4 sets of digits with one ER value" | nso-mob-fp |
| CSCwc83287 | [Smoke2-ICUPS] Undefined_Function_PC and hatsystem_process_card_fail_msg crash seen in regression | pdn-gw |
| CSCwa79744 | BP-ICUPS : CUSP Feature not working in 21.27.x builds | pdn-gw |
| CSCwb66185 | Document: Removal of Step2 under the Generating SSH Client Key Pair | pdn-gw |
| CSCwe17765 | Sgi-reachability handling for permanent disappearance of sessmgr which handles sgi-reachability | pdn-gw |
| CSCwc10201 | Race condition in informing RCM HA state from keepalived to controller | rcm |
| CSCwd91543 | IKE notify packets are not responded after pod reload | rcm |
| CSCwd99902 | Assertion Failures triggered during ADMF provisioning/auditing LI configuration | sae-gw |
| * 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* |
|---|---|---|
| CSCwd39954 | [CUPS-CP] Delay seen when CP handles 32 Sx associated UPs | cups-cp |
| CSCwe00049 | sessmgr memory usage is increasing while number of subscribers remains mostly the same | cups-up |
| CSCwd66766 | cli display shows contradictory information for UP-Group name and UP-NODE-ID | cups-cp |
| CSCwd08502 | [CUPS CP] MBR reduced to 1Kbps during 4G to 3G handoff if 4G AMBR is 4294968 | cups-cp |
| CSCwe24070 | [BP-CUPS]: sessmgr crash at Function: acsmgr_collect_usage_for_all_monitoring_keys() | cups-cp |
| CSCwe01868 | SX collision in Delete IDFT and logs Misc Error3: Internal Failure : SX_MODIFY_REQ failed for Trans | cups-cp |
| CSCwe06468 | CUPS CP: sessmgr restart seen in Function: sgwdrv_pdn_fsm_st_connected_evt_modify_bearer_ind() | cups-cp |
| CSCwd93230 | "[CUPS UP] When dynamic rule precedence is zero, UP is not accounting packet in URR " | cups-up |
| CSCwd67633 | [BP-CUPS]libvnet.so.19.08.1/vlan_ip4_qos_mark_node_fn_avx2() with vpp restart | cups-up |

| Bug ID | Headline | Product Found* |
|---|---|---|
| CSCwd46457 | SSD collection may cause BFD timeout with 16 vpp workers due to show memory main-heap | cups-up |
| CSCwd95901 | "CUPS UP - After sessmgr crash, sessmgr is not showing p2p as loaded in 'show module'" | cups-up |
| CSCwd39197 | E911 calls fail with GTPv2 Cause Code 73 - No Resources Available after PGW fails to send DNS Query | pdn-gw |
| CSCwd65439 | Password change option for user in warning period before expiration. | staros |
| * Information in the "Product Found" column identifies the product in which the bug was initially identified. | | |

# Operator Notes

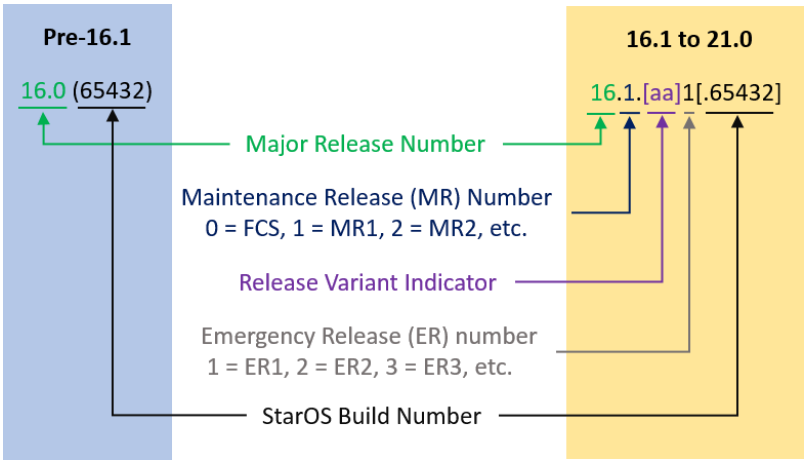
## StarOS Version Numbering System

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.

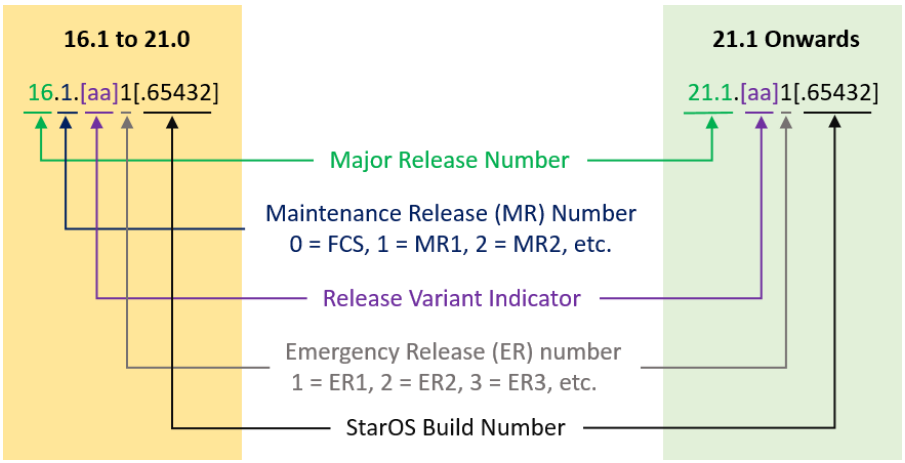
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

| 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.<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>.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. |

| 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.<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 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 6 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 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)