Release Notes for StarOS™ Software Version 21.19.0 and Ultra Service Platform Version N6.13.0

First Published: April 30, 2020
Last Updated: May 11, 2020

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.18.0 and N6.12.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.19.0 build 75571
Ultra Service Platform ISO	10817
usp-em-bundle*	6.12.0, Epoch: 8596
usp-ugp-bundle*	21.19.0, Epoch: 8541
usp-yang-bundle	1.0.0, Epoch: 8560
usp-uas-bundle	6.10.0, Epoch: 8604
usp-auto-it-bundle	5.8.0, Epoch: 8785
usp-vnfm-bundle	4.5.0.112, Epoch: 8561
Ultram Manager	2.11.0, Epoch: 2250
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in Table 3.

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:

- StarOS: https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html
- Ultra Gateway Platform (including the UltraM Solution): https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html
- Ultra Automation Services: https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html
- Virtual Packet Core (including VPC-SI and VPC-DI): https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/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.

Ultra M Hyper-Converged Model Component Version Information

Table 2 - Ultra M Hyper-Converged Model Component Version Information

HW	SW	6.7	6.8	6.9	6.10	6.11	6.12	6.13
	StarOS	71540	72257	72729	73292	73955	74796	75571
	ESC	4.4.0.88	4.5.0.112	4.5.0.112	4.5.0.112	4.5.0.112	4.5.0.112	4.5.0.112
	RH Kernel	7.5	7.5	7.5 or 7.6	7.5 or 7.6	7.5 or 7.6	7.5 or 7.6	7.5 or 7.6
	OSP	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.	10 or 13 **NOTE**: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF-based deployments of the UGP VNF.
UCS C240 M4S SFF (NFVI)	BIOS	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)
	CIMC (BMC)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)	3.0(4d)

HW	SW	6.7	6.8	6.9	6.10	6.11	6.12	6.13
	MLOM	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)	4.1 (3f)
C2960XR-48TD-I (Management)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5	15.2.(2) E5
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.61	7.61
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(4)	7.0(3)I7(4)

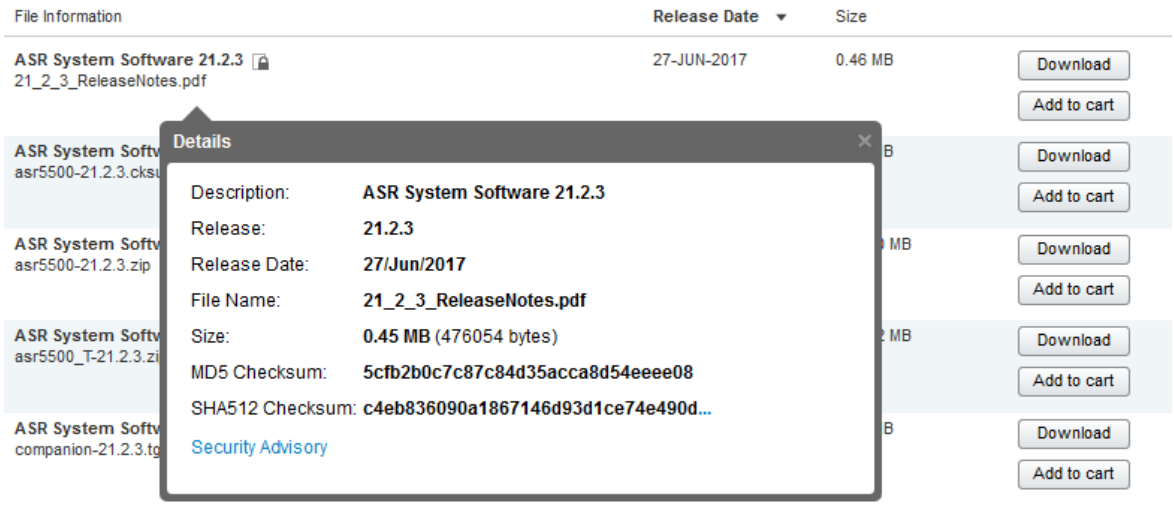
Firmware Updates

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 3 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 3.

Table 3 - 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 4 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvs26391	[BP-CUPS]- sgwdrv_update_bearer_stat()	cups-cp
CSCvu03192	Last Known Location not reported when ISDR is received in UE detached state	mme
CSCvt79109	"[MONTE]: On PDN Connectivity Status, RIA are not incrementing for detach on scef-service statistics"	mme
CSCvt83068	MME doesn't respond to SCEF initiated MT Data and conn release as expected during sessmgr restart	mme
CSCvu03204	Current number of UEs being monitored stats not incremented	mme
CSCvu02977	MME reloads while performing SCEF initiated connection release procedure	mme
CSCvt47005	[BP-Legacy] Traffic allowed despite CCR failure with FHT continue discard traffic post recovery	pdn-gw
CSCvp05787	sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt()	sgsn
* 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 5 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvt46557	"[BP-CUPS]: Assertion failure at egtpc_handle_delete_sess_rsp_evt, lost 50% subs in 2 hours"	cups-cp
CSCvt56799	IPSEC: SX is in Non-Configured state when more than 14 apns are configured	cups-cp
CSCvt49488	In Monsub fastpath packets are captured twice in vpp pcap	cups-up
CSCvt53996	MME returns DIAMETER_ERROR_USER_UNKNOWN for Mon even Number of UE's case	mme
CSCvq00006	MPLS FEC ILM mapping missing for many ip pools after vpnmgr crash	ggsn
CSCvs89155	CDRs have wrong NodeID for AAAMGR instances more than 998.	sgsn
CSCvt12972	Task restart while handling the context response message	sgsn
CSCvp33054	Assertion failure function sn_gt_process_sgsn_dns_query	sgsn
CSCvp12739	show deployment-vnfrs:vnfr command does not work	usp-usf
* Information in the “Product Found” column identifies the product in which the bug was initially identified.		

Operator Notes

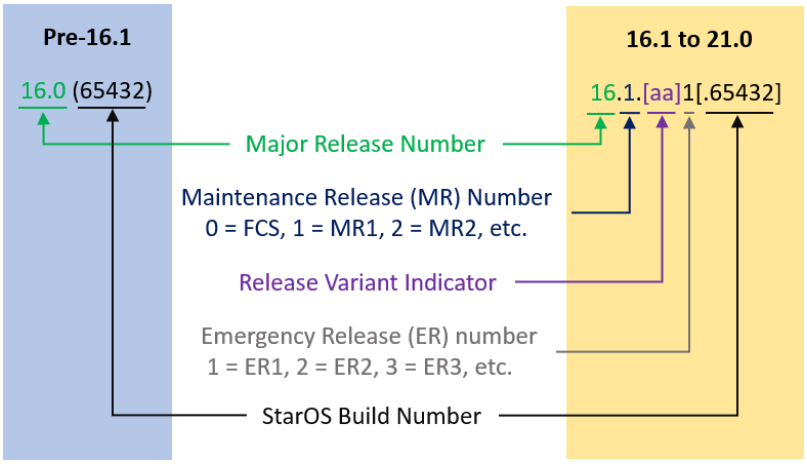
StarOS Version Numbering System

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.

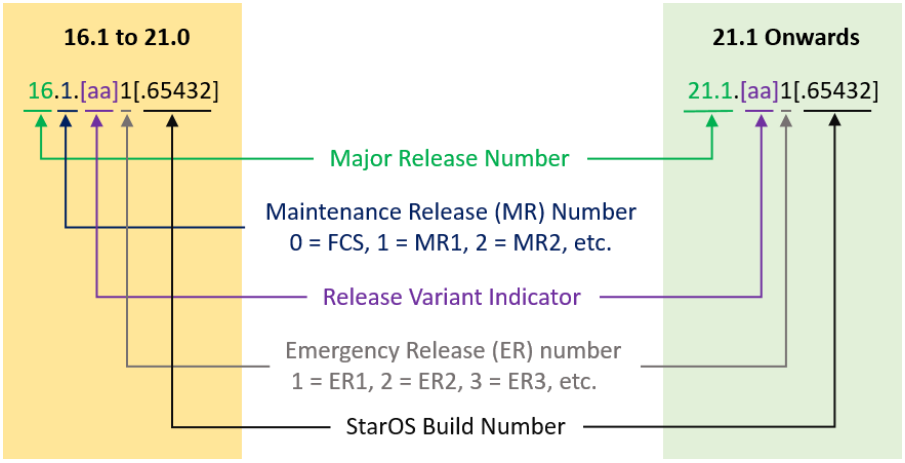
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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 6 provides descriptions for the packages that are available with this release.

Table 6 - 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 7 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 7 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar		Contains information and utilities for verifying USP RPM integrity.

Table 7 - 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.