



Release Notes for StarOS™ Software Version 21.18.0 and Ultra Service Platform Version N6.12.0

First Published: March 6, 2020

Last Updated: March 6, 2020

Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.17.0 and N6.11.0.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.18.0 build 74796
Ultra Service Platform ISO	10694
usp-em-bundle*	6.12.0, Epoch: 8439
usp-ugp-bundle*	21.18.0, Epoch: 8418
usp-yang-bundle	1.0.0, Epoch: 8403
usp-uas-bundle	6.10.0, Epoch: 8481
usp-auto-it-bundle	5.8.0, Epoch: 8628
usp-vnfm-bundle	4.5.0.112, Epoch: 8404
Ultram Manager	2.10.0, Epoch: 1845
* 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	6.6	6.7	6.8	6.9	6.10	6.11	6.12
	StarOS	71244	71540	72257	72729	73292	73955	74796
	ESC	4.4.0.88	4.4.0.88	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	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)

Installation and Upgrade Notes

HW	SW	6.6	6.7	6.8	6.9	6.10	6.11	6.12
	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	7.59	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(3)	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.

The screenshot shows a table of software files with columns for 'File Information', 'Release Date', and 'Size'. A 'Details' popup window is open over the first row, displaying the following information:

- 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

Open Bugs in this Release

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

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](#).

Resolved Bugs in this Release

Table 4 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvs62126	Function restart at egtpc_handle_abort_proc_cmd_evt	cups-cp
CSCvs52657	[SOL TEST] SRP recovery-access-side-failure counters incremented	cups-cp
CSCvt03103	[BP-CUPS] Series of sessmgr reload at function sm restart at sx_handle_user_sap_event	cups-cp
CSCvt03413	Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:735 egtpc_handle_abort_proc_cmd_evt	cups-cp
CSCvt03580	[PLT-CUPS]: Series of [vpn 5013 error] Alloc request received from invalid UP ID =0	cups-cp
CSCvt07835	[BP-CUPS]OCS Unreachable-Action continue/Terminated doesn't increase despite of triggers counter hit	cups-cp
CSCvs03936	CUPS: Segmentation fault at vpn_deregister_user_plane	cups-cp
CSCvt03654	[CUPS] Multiple VPNMGR Crashes during Longevity call model run	cups-up
CSCvs77979	[BP-CUPS] vpnmgr restarts observed during back to back CP switchover	sae-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*
CSCvq69683	[BP-CUPS][IDFT Interactions] Assert at sgwdrv_pdn_fsm_st_newcall_pending_evt_clear_pdn()	cups-cp
CSCvr59193	CUPS: TIME-IDLE in "show sub all" incorrect	cups-cp
CSCvs03936	CUPS: Segmentation fault at vpn_deregister_user_plane	cups-cp
CSCvp19977	"[BP-CUPS]Post UE movement of idle to active, dedicated bearer creation leads to incorrect tep entry."	cups-up
CSCvs58178	[BP CUPS] uplane_drv_fsm_handle_invalid_evt()	cups-up
CSCvt00159	Debug log shows errors with CUSP VPP msgid	cups-up
CSCvr67110	[PLT-ICUPS]: [vpn 5103 error] UDP Med received packet with non-udp protocol on DPC2 card migration	pdn-gw
CSCvs03855	SM restart- sessmgr_handle_sef_async_packet()	pdn-gw
CSCvs14612	License status of Subscriber Firewall Service in over License Capacity	pdn-gw
CSCvs64065	CLI process restart: Fatal Signal 11: Segmentation fault PC: [014b6828/X] cli_print	sae-gw

Operator Notes

Bug ID	Headline	Product Found*
CSCvs60046	ASR5500 sessmgr reloads on saegwdrv_dequeue_from_buffer_queue	sae-gw
CSCvs43940	sessmgr_wifigw_tft_get_subsess_from_tft() ipv4	samog
CSCvt15867	Assertion failure with sessmgr_gprs_process_del_sub_session	sgsn
CSCvr09725	Memory allocated to gbmgr is 0k when SF have 24Gb mem	sgsn
CSCvs24520	sessmgr restarts due to assertion failure at function gmm_acc_abort_req()	sgsn
CSCvs24524	sessmgr restarts due to assertion failure at function sessmgr_collect_sgsn_call_rcvry_info()	sgsn
CSCvs24529	sessmgr restarts due to assertion failure at function pmm_ms_fsm_invalid_event_handler()	sgsn
CSCvs24536	sessmgr restarts due to assertion failure at event PMM_EVT_SM_PMM_PAGING_REQ	sgsn
CSCvs19562	LI Data are sent in the clear over the DI LAN	staros
CSCvs03366	[BP-ICUPS]: npumgr restart observed with call model run	staros
CSCvs40441	TACACS accounting request error messages seen in syslog for prime user expired session	staros
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

StarOS Version Numbering System

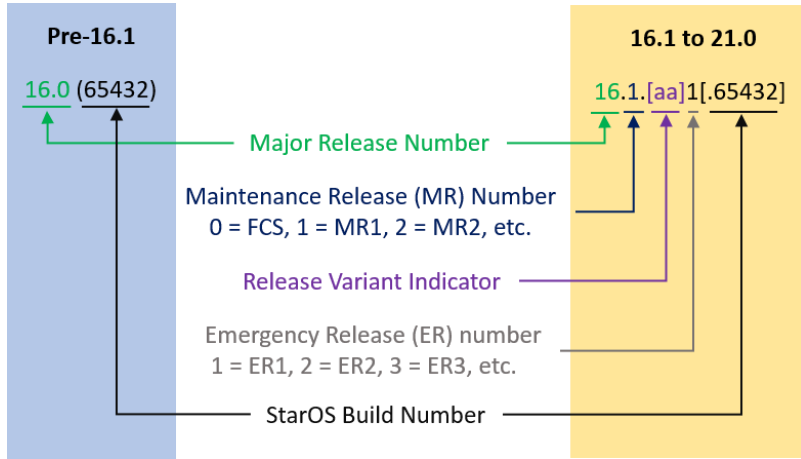
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

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.

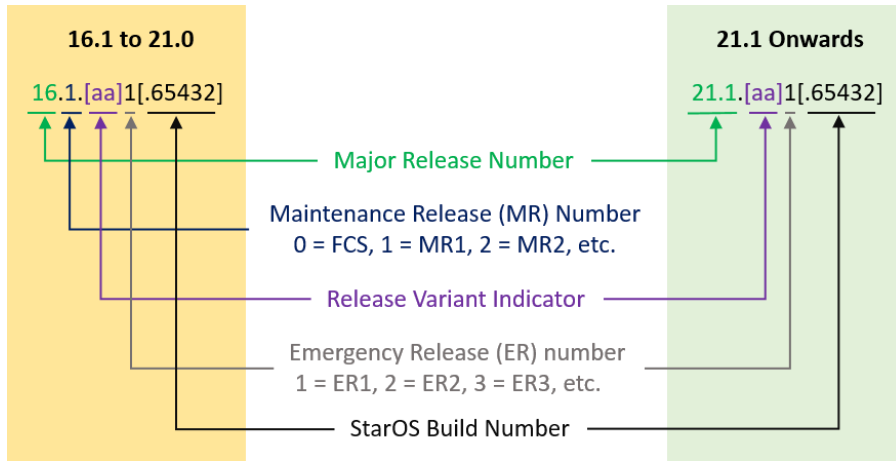
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

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".

Operator Notes



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		

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
companion- <release>.zip	companion- <release>.tgz	<p>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.</p> <p>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.</p>
VPC-DI		
qvmc-di- <release>.bin.zip	qvmc-di-<release>.bin	<p>Contains the VPC-DI 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-di_T- <release>.bin.zip	qvmc-di_T-<release>.bin	<p>Contains the trusted VPC-DI 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-di-<release>.iso.zip	qvmc-di-<release>.iso	<p>Contains the VPC-DI 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-di_T- <release>.iso.zip	qvmc-di_T-<release>.iso	<p>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.</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-<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>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-di-template-libvirt-kvm-<release>.zip	qvmc-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.
qvmc-di-template-libvirt-kvm_T-<release>.zip	qvmc-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.
qvmc-di-<release>.qcow2.zip	qvmc-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.
qvmc-di_T-<release>.qcow2.zip	qvmc-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		
qvmc-si-<release>.bin.zip	qvmc-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.
qvmc-si_T-<release>.bin.zip	qvmc-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.
qvmc-si-<release>.iso.zip	qvmc-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.
qvmc-si_T-<release>.iso.zip	qvmc-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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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>
qvmc-si_T-<release>.qcow2.zip	qvmc-si_T-<release>.qcow2.gz	<p>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.</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 Companion Package		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	<p>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.</p> <p>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.</p>
Ultra Service Platform		

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

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)

© 2020 Cisco Systems, Inc. All rights reserved.