



Release Notes for StarOS™ Software Version 21.12.4

First Published: March 18, 2019

Last Updated: March 18, 2019

Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.12.3. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.12.4, build 71447

Descriptions for the various packages provided with this release are located in [Release Package Descriptions](#).

Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

Refer to the [Release Change Reference](#) for a complete list of feature and behavior changes associated with the software release on which this emergency release is based.

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 installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Firmware Updates

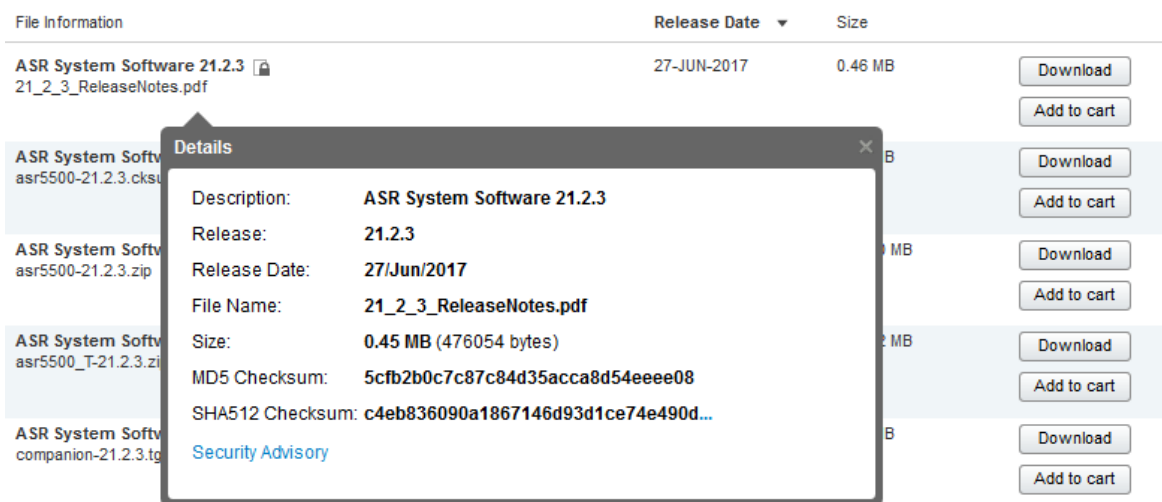
There are no firmware upgrades required for this release.

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 the following mechanisms:

- 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.

- .cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

`<product>-<version>.cksums`

Example: `asr5500-21.4.0.cksums`

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 please see the table below.

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 <code>> certutil.exe -hashfile <filename>.<extension> SHA512</code>

Open Bugs in this Release

Operating System	SHA512 checksum calculation command examples
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/or that 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*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvn80152	[BP-CUPS] Observing new IE Interface: SXa wrongly sent in PFCP Heartbeat Request/Response	cups-cp

Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCvn44898	[PLT-CUPS-VPP] : TCP Flows are not getting cleared after FIN is received	cups-up
CSCvo13488	[BP-CUPS] Sessctrl in 'Over' state with 10k calls	cups-up
CSCvn75110	[BP-CUPS] High memory utilization by sessmgr - probable memory leak	cups-up
CSCvo01375	[CUPS] VPP restart observed with stack libvlib.so.0/unix_cli_file_welcome_timer()	cups-up
CSCvo07207	[BP-CUPS] sessctrl restart in UP	cups-up
CSCvn46872	[BP-CUPS] UP gets stuck when disassociated and associated with new CP with different ECS config	cups-up
CSCvo48775	MME: MEC - Inter-MME S1 HO trigger unexpected detach	mme
CSCvo55100	clear mme-service statistics not clearing Dual Connectivity with NR Subscribers stats	mme
CSCvo15422	mmemgr task restart due to a segmentation in S1ap	mme
CSCvo85261	[BP-ICUPS]:sessmgr restart observed at acsmgr_fp_handle_stream_state_change()	pdn-gw
CSCvn55676	[BP-CUPS]:Uplink Stream remain in Config state after Flow status change	pdn-gw
CSCvo31100	[BP-ICUPS]X3 table entries absent post DMX migration	pdn-gw
CSCvo32237	[BP-ICUPS]: some UDP streams going to passive post ICSR switchover	pdn-gw
CSCvn75072	[BP:ICUPS]:Sessmgr restart@fapi_tp_process_incoming_local_row_req on DPC2 card reboot.	pdn-gw
CSCvo30174	[BP-ICUPS]Unable to get over 4.3 Gbps on HSLI without fifo Q full on threads	pdn-gw
CSCvo37441	wrong firewall Ruledef stats shown in 'show active-charging ruledef statistics all firewall wide'.	pdn-gw
CSCvo32889	"[BP-ICUPS]:sessmgr 0 error fastpath_stream_add(): Stream [Ver: 0, locus: 2, client_id: 8, stats_tabl"	sae-gw
CSCvo36105	[BP-ICUPS]: acsmgr 91369 error Error: Client-Server API: Add conneciton request to Dhost failed	sae-gw

Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvo45264	[BP-ICUPS]: Data is not proper for 5G UE of ipv6 pdntype	sae-gw
CSCvo49923	[BP-ICUPS] Fastpath errors flooding syslog messages on 21.12.0.71244 EFT	sae-gw
CSCvo82068	[BP-ICUPS]: 4G sub with NAT44 fragmented traffic NOT getting charged to Dynamic rule	sae-gw
CSCvi12541	bfdlc facility instances in warn state on active and standby chassis	sae-gw
CSCvo31408	saegw-service stats not updating for CSRsp denied due to license exceeded	sae-gw
CSCvn94523	F2725: Rab Rel Response counters are not pegged	sgsn
CSCvn60293	[BP-CUPS] flow-add-failed count is increased while make and break call is running	staros
CSCvo27835	[BP-ICUPS-saegw-DPC2]: HSLI - intercept failures observed due to tx fifo full	staros
CSCvn79019	[BP-ICUPS] Streams are not getting recovered [BP after Planned DPC2 Migration with 5g calls	staros
CSCvo04967	StarOS cannot assign multiple IPv6 address for diameter peer	staros
CSCvo20944	[BP-ICUPS]: starOS CLI commands are NOT getting logged into configured syslog	staros
* 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*
CSCvm59761	[PLT-CUPS-VPP]IPv6 fragmentation issue	cups-up
CSCvo25826	[PLT-CUPS] [PLT-ICUPS] CUPS VPP task restart observed on UP and VPP task not recovered too	cups-up
CSCvo22218	[BP:ICUPS]:VPP restart at vnet_per_buffer_interface_output_avx2() on call model run	pdn-gw
CSCvo51439	[BP-ICUPS] : EGTPIN-MGR reboots during Socket based SessMgr selection	pdn-gw

Bug ID	Headline	Product Found*
CSCvo70468	[PLT-ICUPS]30 min delay in DPC card switch to standby after vpp component crash	pdn-gw
CSCvo73212	[BP-PLT-ICUPS]: egtpinmgr restart observed during callmodel	pdn-gw
CSCvo70468	[PLT-ICUPS]30 min delay in DPC card switch to standby after vpp component crash	pdn-gw
CSCvo73354	[PLT-ICUPS-VPP] VPP does not start after unplanned card migration following MIO switchover	sae-gw
CSCvo22820	Improvement on Fabric persistdump data collection	sae-gw
CSCvo42844	[PLT-ICUPS] Hundreds of Sessmgr asserts for fapi_tp_restart_notify_internal() on 21.12.0.71244	sae-gw
CSCvo75731	"[BP-ICUPS]: For 4G sub with fragmented UI,DL traffic ECS flows are incorrect"	sae-gw
CSCvo75731	"[BP-ICUPS]: For 4G sub with fragmented UI,DL traffic ECS flows are incorrect"	sae-gw
CSCvo65495	VPP unable to config 40G NIC to retain VLAN tag	staros
CSCvo73630	[BP-PLT-ICUPS]: Unplanned DPC2 failover resulted chassis reload	staros
CSCvo77214	"[PLT-CUPS][BP-PLT-ICUPS]:All 4G/5G subs traffic loss in call model,rx-no-bufinvppctl show interface"	staros
CSCvo72124	[BP-PLT-ICUPS]:rx-miss seen across all worker threads(120) after overnight call model run	staros
CSCvo73350	"[BP-PLT-ICUPS]: All UDP (v6, v4+v6 with v4 NAT) fragmented pkts getting dropped as bad hdr by SM"	staros
CSCvo72124	[BP-PLT-ICUPS]:rx-miss seen across all worker threads(120) after overnight call model run	staros
CSCvo73350	"[BP-PLT-ICUPS]: All UDP (v6, v4+v6 with v4 NAT) fragmented pkts getting dropped as bad hdr by SM"	staros

* Information in the "Product Found" column identifies the product in which the bug was initially identified.

Operator Notes

StarOS Version Numbering System

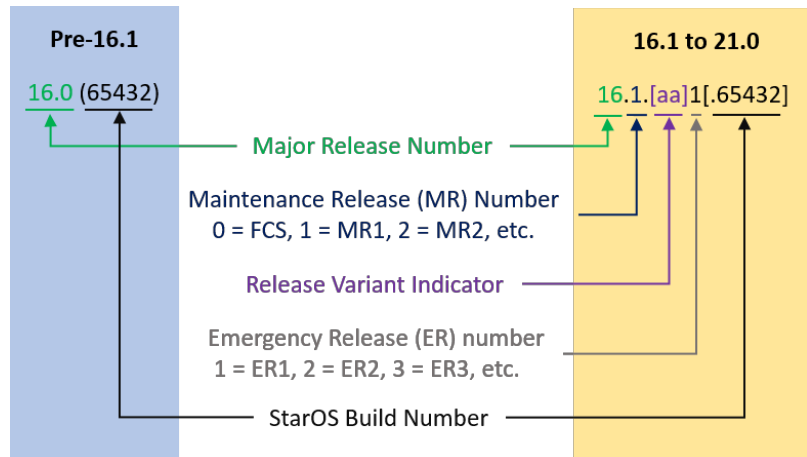
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

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.

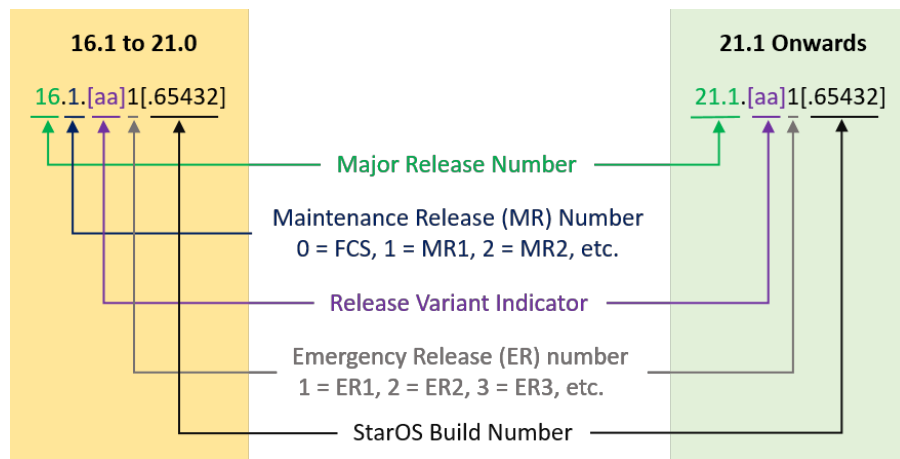
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

Operator Notes

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		

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
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	<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		
qvpc-di- <release>.bin.zip	qvpc-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>
qvpc-di_T- <release>.bin.zip	qvpc-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>
qvpc-di- <release>.iso.zip	qvpc-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>

Operator Notes

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di_T- <release>.iso.zip	qvpc-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>
qvpc-di-template-vmware- <release>.zip	qvpc-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>
qvpc-di-template-vmware_T- <release>.zip	qvpc-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>
qvpc-di-template-libvirt-kvm- <release>.zip	qvpc-di-template-libvirt-kvm- <release>.tgz	<p>Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di-template-libvirt-kvm_T- <release>.zip	qvpc-di-template-libvirt-kvm_T- <release>.tgz	<p>Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-di- <release>.qcow2.zip	qvpc-di- <release>.qcow2.tgz	<p>Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di_T- <release>.qcow2.zip	qvpc-di_T- <release>.qcow2.tgz	<p>Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
VPC-SI		
qvpc-si- <release>.bin.zip	qvpc-si- <release>.bin	<p>Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si_T- <release>.bin.zip	qvpc-si_T- <release>.bin	<p>Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si- <release>.iso.zip	qvpc-si- <release>.iso	<p>Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>
qvpc-si_T- <release>.iso.zip	qvpc-si_T- <release>.iso	<p>Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>

Operator Notes

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		

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

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)

© 2019 Cisco Systems, Inc. All rights reserved.