Cisco Prime Access Registrar 9.3 Release Notes

Cisco Prime Access Registrar (Prime Access Registrar) is a high performance, carrier class, 3GPP-compliant, 64-bit RADIUS/Diameter solution that provides scalable, flexible, intelligent authentication, authorization, and accounting (AAA) services.

Prime Access Registrar comprises a RADIUS/Diameter server designed from the ground up for performance, scalability, and extensibility for deployment in complex service provider environments including integration with external data stores and systems. Session and resource management tools track user sessions and allocate dynamic resources to support new subscriber service introductions.

Note   Prime Access Registrar can be used with Red Hat Enterprise Linux (RHEL) 7.x and 8.8 or CentOS 7.x operating system. Also, Prime Access Registrar is qualified with VMWare ESXi 7.0 Update 3, OpenStack Xena.

Contents

This release note contains the following sections:

System Requirements

This section describes the system requirements to install and use the Prime Access Registrar software.

Table 1 lists the system requirements for Prime Access Registrar 9.3.

Table 1   *Minimum Hardware and Software Requirements for Prime Access Registrar Server*

OS Version	RHEL 7.x and 8.8
	CentOS 7.x
	You must have the 64-bit rpm files for the relevant RHEL versions while installing Prime Access Registrar. For the list of required rpms for the relevant OS versions, see Required 64-bit rpms for Relevant RHEL OS Versions, page 2.
Model	X86
CPU Type	Intel Xeon CPU 2.30 GHz
Processors	4
CPU Speed	2.30 GHz
Memory (RAM)	8 GB
Swap Space	10 GB
Disk Space	1*146 GB

Prime Access Registrar supports JDK versions 1.8.x and 11.x. Also, Prime Access Registrar is qualified with VMWare ESXi 7.0 Update 3, OpenStack Xena.

Note   These are the minimum system requirements to have Prime Access Registrar up and running. This may vary based on the deployments. Please contact your BU team to know the specific system requirements for your deployment.

Required 64-bit rpms for Relevant RHEL OS Versions

rpm	RHEL OS Version 7.x	RHEL OS Version 8.x
brotli	No	Yes
c-ares	Yes	Yes
cyrus-sasl-lib	Yes	Yes
gamin	Yes	Yes
glibc	Yes	Yes
gdome2	Yes	Yes
glib	Yes	Yes
glib2	Yes	Yes
json-c	Yes	Yes
keyutils-libs	Yes	Yes
krb5-libs	Yes	Yes
libbson	No	Yes
libcom_err	Yes	Yes
libcurl	Yes	Yes

rpm	RHEL OS Version 7.x	RHEL OS Version 8.x
libicu	Yes	Yes
libidn2	No	Yes
libgcc	Yes	Yes
libmongocrypt	No	Yes
libnghttp2	No	Yes
libnsl	No	Yes
libpsl	No	Yes
libselinux	Yes	Yes
libssh	No	Yes
libstdc++	Yes	Yes
libtool-ltdl	Yes	Yes
libunistring	No	Yes
libxcrypt	No	Yes
libxml2	Yes	Yes
libzstd	No	Yes
lksctp-tools	Yes	Yes
mongo-c-driver-libs	No	Yes
ncurses-libs	Yes	Yes
nss-softokn-freebl	Yes	Yes
nss-util	Yes	Yes
nspr	Yes	Yes
nss	Yes	Yes
openldap	No	Yes
openssl-libs	Yes	Yes
pcre	Yes	Yes
pcre2	No	Yes
pcre-cpp	No	Yes
snappy	No	Yes
sqlite-libs	No	Yes
tcl	No	Yes
unixODBC	No	Yes
xz-libs	No	Yes
zlib	Yes	Yes

Co-Existence With Other Network Management Applications

To achieve optimal performance, Prime Access Registrar should be the only application running on a given server. In certain cases, when you choose to run collaborative applications such as a SNMP agent, you must configure Prime Access Registrar to avoid UDP port conflicts. The most common conflicts occur when other applications also use ports 2785 and 2786. For more information on SNMP configuration, see the "Configuring SNMP" section in the "Configuring Cisco Prime Access Registrar" chapter of the *Cisco Prime Access Registrar 9.3 Administrator Guide*.

New and Enhanced Features in Cisco Prime Access Registrar 9.3

Cisco Prime Access Registrar 9.3 provides the following features:

- Migration of GUI Framework, page 4
- Strong Password Policy, page 4

Migration of GUI Framework

The graphical user interface (GUI) for Prime Access Registrar has been upgraded to Angular Spring Boot framework to address the security vulnerabilities with the existing Struts framework. All the GUI features are maintained intact with the current migration.

Strong Password Policy

Following are the criteria that an admin user password should meet as per the strong password policy settings in Prime Access Registrar.

The password must:

- contain at least 8 characters (12+ recommended)
- contain at least one uppercase letter and at least one lowercase letter
- contain at least one numerical value
- contain at least one special character (! ? # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~)
- NOT contain space

Also, we recommend that the password:

- does not contain more than two identical characters in a row
- does not contain first name, last name, email address mailbox or domain, or company name
- does not match commonly used passwords or password character patterns

> **Note**   While upgrading from an existing version to Prime Access Registrar 9.3, all admin user passwords will be reset to the default password *Aicuser@123*.

Cisco Prime Access Registrar 9.3 Bugs

For information on a specific bug or to search all bugs in a particular Prime Access Registrar release, see Using the Bug Search Tool, page 8

This section contains the following information:

- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.6, page 5
- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.5, page 5
- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.4, page 6
- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.3, page 7
- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.2, page 7
- Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.1, page 7

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.6

Table 2 lists the anomalies fixed in Prime Access Registrar 9.3.0.6 release.

Table 2　　　*Fixed Anomalies in Prime Access Registrar 9.3.0.6*

Bug	Description
CSCwj98146	Vulnerabilities in tomcat 9.0.85
CSCwj98139	Vulnerabilities in curl 8.6.0
CSCwj98133	Vulnerabilities in libxml2 2.7.6
CSCwk24022	CPAR sending default and undesired values to BNG

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.5

Table 3 lists the anomalies fixed in Prime Access Registrar 9.3.0.5 release.

Table 3　　　*Fixed Anomalies in Prime Access Registrar 9.3.0.5*

Bug	Description
CSCwj77321	Version change from 9.3.0.4 to 9.3.0.5
CSCwj19541	Vulnerabilities in pcre 8.32
CSCwj60651	Evaluation of cnsar for HTTP/2 CONTINUATION Attack vulnerability
CSCwj19557	CIAM: Vulnerabilities in curl 7.86.0
CSCwj58776	Apache Tomcat upgrade from 9.0.85 to 9.0.87
CSCwj19544	Vulnerabilities in sqlite 3.40.0
CSCwj19563	Vulnerabilities in net-snmp 5.9
CSCwj19535	Vulnerabilities in c-ares 1.18.1

Table 3   ***Fixed Anomalies in Prime Access Registrar 9.3.0.5***

Bug	Description
CSCwj19542	Vulnerabilities in spring-framework 5.3.18
CSCwj19540	Vulnerabilities in snake-yaml 1.29
CSCwj19539	Vulnerabilities in jackson-databind 2.13.2.2
CSCwj19545	Vulnerabilities in tomcat 9.0.60
CSCwj19513	CIAM: Vulnerabilities in openssl 1.1.1n
CSCwj19538	Upgrade old guava version to guava-33.0.0-jre

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.4

Table 4 lists the anomalies fixed in Prime Access Registrar 9.3.0.4 release.

Table 4   ***Fixed Anomalies in Prime Access Registrar 9.3.0.4***

Bug	Description
CSCwh88632	Evaluation of cnsar for HTTP/2 Rapid Reset Attack vulnerability
CSCwi25169	Framed-IPv6-Prefix needs to supported from REST API
CSCwh84603	Core file : CommonSessionManager::releaseAcquiredSession This crash was seen in performance test and it is fixed through this CDET.
CSCwi51551	Core file : LocalSessionManager::acquireSession This crash was seen in performance test and it is fixed through this CDET.
CSCwi51598	Core file : AttributeDictionary::getValue (SIGABRT) This crash was seen in performance test and it is fixed through this CDET.
CSCwi51570	Core file : DiaPeer::getInterfaceIndex (SIGSEGV) This crash was seen in performance test and it is fixed through this CDET.
CSCwi89228	Support for creating an empty userGroup through REST API
CSCwi95109	Apache Tomcat upgrade from 9.0.82 to 9.0.85
CSCwi59344	Spring Core Upgrade 5.6.2 to 5.6.9
CSCwi60587	OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <=20.0.0 Multiple Vulnerabilities OpenJDK upgraded to 8u392
CSCwi69748	Log4J Vulnerability - Update from 2.17 to 2.19

Table 4   ***Fixed Anomalies in Prime Access Registrar 9.3.0.4***

Bug	Description
CSCwi69750	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities Oracle Java SE upgraded to 1.8.0_391
CSCwi06502	Vulnerabilities in jettison 1.3.3 Jettison upgraded from 1.3.3 to 1.5.4
CSCwi91082	Copyright year changed from 2023 to 2024
CSCwj05345	Disable week HMAC algorithms; Disable static key cipher suites; Enable strong ciphers
CSCwi97478	CPAR 7.x build issue fix

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.3

Table 5 lists the anomalies fixed in Prime Access Registrar 9.3.0.3 release.

Table 5   ***Fixed Anomalies in Prime Access Registrar 9.3.0.3***

Bug	Description
CSCwf53731	Memory leak observed while handling OCI service traffic.

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.2

Table 6 lists the anomalies fixed in Prime Access Registrar 9.3.0.2 release.

Table 6   ***Fixed Anomalies in Prime Access Registrar 9.3.0.2***

Bug	Description
CSCwe95813	In encrypted IMSI, private key decryption failed.

Fixed Anomalies in Cisco Prime Access Registrar 9.3.0.1

Table 7 lists the anomalies fixed in Prime Access Registrar 9.3.0.1 release.

Table 7   ***Fixed Anomalies in Prime Access Registrar 9.3.0.1***

Bug	Description
CSCwa27878	Prime Access Registrar stops working on longevity when ErrorBasedRouting is FALSE.

Table 7 **Fixed Anomalies in Prime Access Registrar 9.3.0.1**

Bug	Description
CSCwc37825	carServerSessionUsage counter is not getting updated properly.
CSCwc50844	Prime Access Registrar stops working due to synchronization issues during Mutex lock.

Using the Bug Search Tool

Use the Bug Search tool (BST) to get the latest information about Cisco Prime Access Registrar bugs. BST allows partners and customers to search for software bugs based on product, release, and keyword, and it aggregates key data such as bug details, product, and version.

BST allows you to:

- Quickly scan bug content
- Configure e-mail notifications for updates on selected bugs
- Start or join community discussions about bugs
- Save your search criteria so you can use it later

When you open the Bug Search page, check the interactive tour to familiarize yourself with these and other Bug Search features.

Step 1 Log into the Bug Search Tool.

    a. Go to https://tools.cisco.com/bugsearch.

    b. At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 2 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 3 To search for bugs in a particular release:

    a. In the Search For field, enter the product name and the release version, e.g. Cisco Prime Access Registrar 9.3, and press **Return**. (Leave the other fields empty.)

    b. When the search results are displayed, use the filter and sort tools to find the types of bugs you are looking for. You can search for bugs by severity, by status, how recently they were modified, according to the number of support cases associated with them, and so forth.

Related Documentation

For a complete list of Cisco Prime Access Registrar documentation, see the *Cisco Prime Access Registrar 9.3 Documentation Overview*.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.