Cisco Prime Access Registrar 9.1 Release Notes

Cisco Prime Access Registrar (Prime Access Registrar) is a high performance, carrier class, 3GPP-5G-DNAAA 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) version 6.6 and above and CentOS version 6.5 and above.

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 9.1.

Cisco Systems, Inc.
www.cisco.com

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

OS version	RHEL 6.6 and above CentOS 6.5 and above **Note** Prime Access Registrar supports OpenStack Stein version.
Model	X86
CPU type	Intel Xeon CPU 2.30 GHz
CPU Number	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 1.7 and 1.8 from release 7.3 onwards and version 1.11 from release 9.1 onwards. Also, Apache Tomcat version has been upgraded to 9.0.31.

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 9.1 Administrator Guide*.

New and Enhanced Features in Cisco Prime Access Registrar 9.1

Cisco Prime Access Registrar 9.1 provides the following features:

PLR/SLR Support with Smart Licensing

Support for Permanent License Reservation (PLR)

If your devices cannot access the Internet for security reasons, you can optionally request permanent licenses for each Prime Access Registrar. Permanent license reservation (PLR) is a set of capabilities that is designed for highly secure environments, where communication with outside environment is impossible.

Permanent licenses do not require periodic access to the License Authority. Like PAK licenses, you can purchase a license and install the license key for Prime Access Registrar. You can easily switch between regular smart licensing mode and PLR mode. Prime Access Registrar can operate normally without ongoing communication with either the CSSM or the Smart Software Satellite (on-site collector).

A single “Universal” license PID that authorizes all possible product functionalities will be available, including an unlimited quantity of counted licenses as well.

Support for Specific License Reservation (SLR)

At a high level, Specific License Reservation (SLR) is an enforced licensing model that is similar to node locked licensing. When you activate Prime Access Registrar, there is one-time manual exchange of information with the CSSM as part of product authorization and configuration. No further interaction with the CSSM or Smart Software Satellite is required.

The main difference between PLR and SLR is, SLR allows you to select the required licenses, whereas with PLR it is a single license that activates all the functionalities of the product.

For SLR, all the licenses that are present for smart account are applicable.

For more details about Smart Licensing and PLR/SLR support, see the “Smart Licensing” chapter of the *Cisco Prime Access Registrar 9.1 Installation Guide*.

Diameter Overload Indication Conveyance Support for Diameter

Diameter Overload Indication Conveyance (DOIC) is a set of standards for supporting dynamic overload controls between Diameter servers and Diameter clients. This allows Diameter servers to send overload reports to Diameter clients requesting reduction in traffic (throttling) for any duration of time.

Currently Prime Access Registrar has an application-wide throttling mechanism, in which the application starts dropping packets when the incoming request rate is growing above the configured value. Here all the packets are given equal priority. It is not possible to throttle any specific packets.

With the DOIC feature, under active overload conditions, it is possible to throttle (forward, divert, or drop) the packets based on configured priority levels.

The GUI and CLI are updated to accommodate this feature. For more details, see *Cisco Prime Access Registrar 9.1 User Guide*.

Enhanced Health Monitoring in Prime Access Registrar

Prime Access Registrar supports regular health monitoring for RADIUS server. A new parameter **EnableHealthMonitoring** is introduced to support enhanced health monitoring for RADIUS and Diameter.

You can monitor the health of Prime Access Registrar server using the following parameters:

- CPU Utilization

- Memory
- Packet Buffer
- Worker Threads count
- Packet Rejects
- Packet Drops
- Packet Time Outs
- Peer Connectivity

All the above parameters are displayed by using the **health** command in CLI.

You have an option to set threshold limits against which the individual health check parameters are monitored. The threshold limits are entered in percentage unit. You can also set the monitoring frequency.

When these health check parameters hit the threshold limit, corresponding warning, error, and reset traps are triggered and the health status is captured as part of the statistics.

The GUI and CLI are updated to accommodate this feature. For more details, see the *Cisco Prime Access Registrar 9.1 User Guide* and *Cisco Prime Access Registrar 9.1 Reference Guide*.

Equipment Identity Registrar (EIR) Check Support in Prime Access Registrar

The Mobile Equipment Identity is used between the 3GPP AAA Server and the Equipment Identity Registrar (EIR) to check the identity status of a Mobile Equipment (ME) for e.g. to ensure the ME is not stolen or verify that the ME has no faults. This procedure is mapped to the commands ME-Identity-Check-Request/Answer (ECR/ECA).

In SWm interface, the IMEI number is retrieved by ePDG from the client and is sent in the Terminal-Information AVP of the DER packet.

In STa interface, Prime Access Registrar retrieves the IMEI information using additional AVPs in the EAP call flows.

The GUI and CLI are updated to accommodate this feature. For more details, see the *Cisco Prime Access Registrar 9.1 User Guide* and *Cisco Prime Access Registrar 9.1 Reference Guide*.

Core Network Restrictions AVP support

The following counters are added to support core network restrictions in Prime Access Registrar:

Diameter Peers

- cdbpPeerStatsCoreNetRestrictionDEAsIn—Number of DEA messages with **Core-Network-Restrictions** AVP that are received from the peer. The Core-Network-Restrictions AVP is present in the DEA packet to indicate the various types of core networks that are not allowed for a given user.
- cdbpPeerStatsCoreNetRestrictionDEAsOut—Number of DEA messages with Core-Network-Restrictions AVP that are sent to the peer.

Diameter Remote Servers

- cDiaRemSvrStatsCoreNetRestrictionSAAsIn—Number of SAA messages with Core-Network-Restrictions AVP that are received by the remote server. The Core-Network-Restrictions AVP is present in the Non-3GPP-User-Data of SAA packet and contains a bitmask indicating the types of core networks that are not allowed for a given user.
- cDiaRemSvrStatsCoreNetRestrictionSAAsOut—Number of SAA messages with Core-Network-Restrictions AVP that are sent by the remote server.
- cDiaRemSvrStatsCoreNetRestrictionFailedSARs—Number of failed SAR messages with Core-Network-Restrictions AVP that are received by the remote server.
- cDiaRemSvrStatsCoreNetRestrictionFailedDERs—Number of failed DER messages with Core-Network-Restrictions AVP that are received by the remote server.

Diameter Stale Session Thread Monitoring Support

The following traps are introduced for monitoring Diameter stale session thread:

- carStaleSessionRemovalThreadStoppedTrap—carStaleSessionRemovalThreadStoppedTrap is generated when stale session removal thread stops working for diameter session manager of type Local.
- carSessionRestorationThreadStoppedTrap—carSessionRestorationThreadStoppedTrap is generated when session restoration thread stops working for diameter session manager of type Local.
- carDiaPacketSizeErr—carDiaPacketSizeErr trap is generated when Prime Access Registrar receives Diameter Packet with packet size that exceeds the configured **DiameterPacketSize** value.

Note You must set **EnableDiaPacketSizeTrap** to **TRUE** under **/radius/advanced/SNMP** to receive the **carDiaPacketSizeErr** trap.

REST API Support for COA Using with-profile Option

Prime Access Registrar supports REST API for Change of Authorization (CoA) using **with-profile** option along with the existing parameters.

The parameters supported for REST API for CoA with-profile option are: **with-ID**, **with-NAS**, **with-User**, **with-Key**, **with-IP-Address**, **with-IP-Subnet**, **with-IPX-Network**, **with-USR-VPN**, **with-Home-Agent**, **with-Age**, and **with-Attribute**.

Prime Access Registrar supports **send-CoA** using CLI and REST API interfaces. For configuring **send-CoA** using CLI, see the “query-sessions” section in the “Setting the Cisco Prime Access Registrar Configurable Option” chapter of the *Cisco Prime Access Registrar 9.1 Administrator Guide*. For configuring **send-CoA** using REST API, see the “CoA and PoD REST APIs” section in the “Support for REST API in Cisco Prime Access Registrar 9.1” chapter of the *Cisco Prime Access Registrar 9.1 Reference Guide*.

To know about configuring CoA requests, refer to the “Using Cisco Prime Access Registrar Server Features” chapter of the *Cisco Prime Access Registrar 9.1 User Guide*.

Cisco Prime Access Registrar 9.1 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.

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 9.1, 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 9.1 Documentation Overview*.

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

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)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.