
# Overview

The chapter provides an overview of the RADIUS server, including connection steps, RADIUS message types, and using Cisco Prime Access Registrar (Prime Access Registrar) as a proxy server.

Prime Access Registrar is a 3GPP-compliant, 64-bit carrier-class RADIUS (Remote Authentication Dial-In User Service)/Diameter server that enables multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

Prime Access Registrar handles the following tasks:

- Authentication—determines the identity of users and whether they can be allowed to access the network
- Authorization—determines the level of network services available to authenticated users after they are connected
- Accounting—keeps track of each user's network activity
- Session and resource management—tracks user sessions and allocates dynamic resources

Using a RADIUS server allows you to better manage the access to your network, as it allows you to store all security information in a single, centralized database instead of distributing the information around the network in many different devices. You can make changes to that single database instead of making changes to every network access server in your network.

Prime Access Registrar also allows you to manage the complex interconnections of the new network elements in order to:

- adequately manage the traffic
- perform appropriate load balancing for desired load distribution
- allow binding of different protocol interfaces corresponding to a subscriber/network element

Service providers transform their 3G and 4G wireless networks with complex services, tiered charging, converged billing, and more by introducing increasing numbers and types of Diameter-based network elements. LTE and IMS networks are the most likely to implement these new network elements—including Policy and Charging Rules Functions (PCRF), Home Subscriber Servers (HSS), Mobility Management Entities (MME), Online Charging Systems (OCS), and others. As a result, as the traffic levels grow, these wireless networks are becoming more difficult to manage and scale without the Prime Access Registrar infrastructure.

Prime Access Registrar allows GUI-based, CLI-based, and REST API-based configurations. For more details, see the "Using the Graphical User Interface" chapter of the *Cisco Prime Access Registrar 9.0 User Guide,* the "Using the aregcmd Commands" chapter of the *Cisco Prime Access Registrar 9.0 Administrator Guide*, and Chapter D, "REST API Framework."

This chapter contains the following sections:

# Prime Access Registrar Directory Structure

The installation process populates the **/opt/CSCOar** directory with the subdirectories listed in Table 1-1.

***Table 1-1 /opt/CSCOar Subdirectories***

| Subdirectory | Description |
|---|---|
| **.system** | Contains ELFs, or binary SPARC executables that should not be run directly. |
| **bin** | Contains shell scripts and programs frequently used by a network administrator; programs that can be run directly. |
| **conf** | Contains configuration files. |
| **data** | Contains the **radius** directory, which contains session backing files; and the **db** directory, which contains configuration database files. |
| **examples** | Contains documentation, sample configuration scripts, and shared library scripts. |
| **lib** | Contains Prime Access Registrar software library files. |
| **logs** | Contains system logs and is the default directory for RADIUS accounting. |
| **odbc** | Contains Prime Access Registrar ODBC files. |
| **scripts** | Contains sample scripts that you can modify to automate configuration, and to customize your RADIUS server. |
| **temp** | Used for temporary storage. |
| **ucd-snmp** | Contains the UCD-SNMP software Prime Access Registrar uses. |
| **usrbin** | Contains a symbolic link that points to **bin.** |

# Program Flow

When a NAS sends a request packet to Prime Access Registrar with a name and password, Prime Access Registrar performs the following actions. Table 1-2 describes the flow without regard to scripting points.

***Table 1-2 From Access-Request to Access-Accept***

| Prime Access Registrar Server Action | Explanation |
|---|---|
| Receives an Access-Request | The Prime Access Registrar server receives an Access-Request packet from a NAS. |
| Determines whether to accept the request | The Prime Access Registrar server checks to see if the client's IP address is listed in **/Radius/Clients/**<*Name*>/<*IPAddress*>. |

*Table 1-2 From Access-Request to Access-Accept (continued)*

| Prime Access Registrar Server Action | Explanation |
|---|---|
| Invokes the policy SelectPolicy if it exists | The Prime Access Registrar Policy Engine provides an interface to define and configure a policy and to apply the policy to the corresponding access-request packets. |
| Performs authentication and/or authorization | Directs the request to the appropriate service, which then performs authentication and/or authorization according to the type specified in **/Radius/Services/**<*Name*>**/**<*Type*>. |
| Performs session management | Directs the request to the appropriate Session Manager. |
| Performs resource management for each Resource Manager in the SessionManager | Directs the request to the appropriate resource manager listed in **/Radius/SessionManagers/**<*Name*>**/**<*ResourceManagers*>**/**<*Name*>, which then allocates or checks the resource according to the type listed in **/Radius/**<*ResourceManagers*>**/**<*Name*>**/**<*Type*>. |
| Sends an Access-Accept | Creates and formats the response, and sends it back to the client (NAS). |

Prime Access Registrar supports Diameter with Extensible Authentication Protocol (EAP) functionality to enable authentication between NAS and a backend NAS Diameter authentication server. For more information, see the "Diameter" chapter of the *Cisco Prime Access Registrar 9.0 User Guide*.

Prime Access Registrar also support 3GPP compliance by implementing a set of protocols. To understand more about the 3GPP AAA server support and the call flow, see the "Wireless Support" chapter of the *Cisco Prime Access Registrar 9.0 Reference Guide*.

# Scripting Points

Prime Access Registrar lets you invoke scripts you can use to affect the Request, Response, or Environment dictionaries. This section contains the following topics:

- Client Scripting
- Client or NAS Scripting Points
- Authentication and/or Authorization Scripting Points

## Client Scripting

Though Prime Access Registrar allows external code (Tcl/C/C++/Java) to be used by means of a script, custom service, policy engine, and so forth, while processing request, response, or while working with the environment dictionaries, it shall not be responsible for the scripts used and will not be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of the script.

Prime Access Registrar also allows you to define internal scripts, by which you can add, modify, or delete attributes in the request, response, and environment dictionaries for RADIUS, Diameter, and TACACS+.

## Client or NAS Scripting Points

Table 1-3 shows the location of the scripting points within the section that determines whether to accept the request from the client or NAS. Note, the scripting points are indicated with the asterisk (*) symbol.

***Table 1-3 Client or NAS Scripting Points***

| Action | Explanation |
|---|---|
| Receives an Access-Request. | The Prime Access Registrar RADIUS server receives an Access-Request packet from a NAS. |
| Determines whether to accept the request. | The client's IP address listed in **/Radius/Clients/**<*Name*>**/IPAddress.** |
| *Executes the server's incoming script. | A script referred to in **/Radius/IncomingScript.** |
| *Executes the vendor's incoming script. | The vendor listed in /Radius/Clients/*Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript.** |
| *Executes the client's incoming script. | A script referred to in **/Radius/Clients/**<*Name*>**/IncomingScript.** |
| Determines whether to accept requests from this specific NAS. | |
| | **/Radius/Advanced/RequireNASsBehindProxyBeInClientList** set to TRUE. |
| | The NAS's Identifier listed in **/Radius/Clients/**<*Name*>, or its NAS-IP-Address listed in **/Radius/Clients/**<*Name*>**/IPAddress.** |
| **If the client's IP address listed in /Radius/Clients/**<*Name*>**/IPAddress is different:** | |
| *Executes the vendor's incoming script. | The vendor listed in **/Radius/Clients/***Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript.** |
| *Executes the client's incoming script. | The client listed in the previous /Radius/Clients/*Name*, and is a script referred to in /Radius/Clients/*Name*/IncomingScript. |

## Authentication and/or Authorization Scripting Points

Table 1-4 shows the location of the scripting points within the section that determines whether to perform authentication and/or authorization.

***Table 1-4 Authentication and Authorization Scripting Points***

| Action | Explanation |
|---|---|
| Determines Service to use for authentication and/or authorization. | The Service name defined in the Environment dictionary variable **Authentication-Service**, and is the same as the Service defined in the Environment dictionary variable **Authorization-Service**. |
| | The Service name referred to by **/Radius/DefaultAuthenticationService**, and is the same as the Service defined in **/Radius/DefaultAuthorizationService**. |
| Performs authentication and/or authorization. | If the Services are the same, perform authentication and authorization. |
| | If the Services are different, just perform authentication. |

*Table 1-4 Authentication and Authorization Scripting Points (continued)*

| Action | Explanation |
|---|---|
| *Executes the Service's incoming script. | A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**. |
| Performs authentication and/or authorization. | Based on the Service type defined in **/Radius/Services/**<*Name*>**/**<*Type*>. |
| *Executes the Service's outgoing script. | A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**. |
| Determines whether to perform authorization. | The Service name defined in **/Radius/DefaultAuthorizationService**, if different than the Authentication Service. |
| *Executes the Service's incoming script. | A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**. |
| Performs authorization. | Checks that the Service type is defined in **/Radius/Services/**<*Name*>**/**<*Type*>. |
| *Executes the Service's outgoing script. | A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**. |

# Script Processing Hierarchy

For request packets, the script processing order is from the most general to the most specific. For response packets, the processing order is from the most specific to the most general.

Table 1-5, Table 1-6, and Table 1-7 show the overall processing order and flow: (1-6) Incoming Scripts, (7-11) Authentication/Authorization Scripts, and (12-17) Outgoing Scripts.

**Note** The client and the NAS can be the same entity, except when the immediate client is acting as a proxy for the actual NAS.

*Table 1-5 Prime Access Registrar Processing Hierarchy for Incoming Scripts*

| Overall Flow Sequence | Incoming Scripts |
|---|---|
| 1) | Radius. |
| 2) | Vendor of the immediate client. |
| 3) | Immediate client. |
| 4) | Vendor of the specific NAS. |
| 5) | Specific NAS. |
| 6) | Service. |

*Table 1-6 Prime Access Registrar Processing Hierarchy for Authentication/Authorization Scripts*

| Overall Flow Sequence | Authentication/Authorization Scripts |
|---|---|
| 7) | Group Authentication. |
| 8) | User Authentication. |
| 9) | Group Authorization. |
| 10) | User Authorization. |
| 11) | Session Management. |

*Table 1-7 Prime Access Registrar Processing Hierarchy for Outgoing Script*

| Overall Flow Sequence | Outgoing Scripts |
|---|---|
| 12) | Service. |
| 13) | Specific NAS. |
| 14) | Vendor of the specific NAS. |
| 15) | Immediate client. |
| 16) | Vendor of the immediate client. |
| 17) | Radius. |

# Service and Ports Used in Prime Access Registrar

## Secure Shell Service

SSH Daemon(SSHD) is the daemon program which is used for ssh(1). It provides secure shell encrypted communications between two hosts over network.

In case of Prime Access Registrar, SSH is used to connect to Prime Access Registrar server and configure Prime Access Registrar using CLI.

## Ports

The following table lists the port numbers that are used for various services in Prime Access Registrar for AAA.

*Table 1-8 Ports Used in Prime Access Registrar*

| Names | Description | Port Numbers | Service of the Ports | Access from Network Node | Configuration Setting | Protocol Name and Reference |
|---|---|---|---|---|---|---|
| AR AAA Service | The RADIUS packet listener uses these ports by default. | 1812-udp | RADIUS AA | Network Access Server | You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI. | RADIUS AA (Authentication, and Authorization) service. |
| | | 1813-udp radacct | RADIUS Accounting | Network Access Server | You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI. | RADIUS Accounting service.<br>Refer to RFC 6733 for more information. |
| | | 3799/udp | RADIUS Dynamic Authorization (CoA/PoD) | Network Access Server | N/A | RADIUS Dynamic authorization which is used with (CoA/PoD) packet types. |
| AR AAA Service | The TACACS+ packet listener uses this port by default. | 49/tcp | TACACS+ | Network Access Server | You can change the default or define new RADIUS port numbers under */Radius/Advanced/Ports* in the CLI and *Configuration > Advanced > Ports* in the GUI. | TACACS+ based on AAA service (Authentication, Authorization, and Accounting).<br>Refer to RFC 1491 for more information. |

*Table 1-8 Ports Used in Prime Access Registrar (continued)*

| Names | Description | Port Numbers | Service of the Ports | Access from Network Node | Configuration Setting | Protocol Name and Reference |
|---|---|---|---|---|---|---|
| AR AAA Service | The DIAMETER packet listener uses these ports by default. | 3868/tcp | DIAMETER | Network Access Server | You can enable or disable this service in *Radius/Advanced/Diameter/IsDiameterEnabled*. | DIAMETER AA Service (Authentication, and Authorization) by tcp protocol.<br>Refer to RFC 4005 for more information. |
| | | 3868/sctp | DIAMETER | Network Access Server | You can enable or disable this service in *Radius/Advanced/Diameter/IsDiameterEnabled*[1]. | DIAMETER AA Service (Authentication, and Authorization) by SCTP protocol. |
| AR MCD Server | MCD is used to store Prime Access Registrar configuration. | 2786/tcp | MCD database Server | This service can be accessed from local host by Prime Access Registrar radius and server agent process. | N/A | Proprietary IPC mechanism. |
| AR Server Agent | AR Server Agent is used to log all the activities of Prime Access Registrar processes. | 2785/tcp | Internal IPC mechanism | This service can be accessed from local host by Prime Access Registrar radius and server agent process. | N/A | Proprietary IPC mechanism. |

*Table 1-8 Ports Used in Prime Access Registrar (continued)*

| Names | Description | Port Numbers | Service of the Ports | Access from Network Node | Configuration Setting | Protocol Name and Reference |
|---|---|---|---|---|---|---|
| AR GUI Service | Prime Access Registrar GUI processes use these ports by default. | 8080/tcp | AR HTTP service | This service is accessible from any end user desktop browser using http protocol. | You can change the default port numbers in editing the *server.xml* file. | Standard HTTP protocol |
| | | 8443/tcp | AR HTTPS service | This service is accessible from any end user desktop browser using https protocol. | You can change the default port numbers in editing the *server.xml* file. | Standard HTTPS protocol |
| | | 8005/tcp | Internally used by Apache Tomcat container | Local host | You can change the default port numbers in editing the *server.xml* file.. | To shutdown Tomcat JVM service instance. |
| | | 8009/tcp | Apache Tomcat container<br>AJP 1.3 Connector | Local host | You can change the default port numbers in editing the *server.xml* file. | Apache JServ protocol.<br>AJP 1.3 Connector. |
| SNMP Master Agent | SNMP Packet listener supports these ports by default. | 161/udp | Simple Net Management Protocol | This service is accessible from any network management host. | Refer to net-snmp documentation for more information. | SNMP MIBs server |
| | | 162/udp | Traps for SNMP | This service is accessible to any SNMP trap client when you want to use net-snmp snmptrap daemon as a SNMP trap server. | Refer to SNMP chapter of the *Cisco Prime Access Registrar 9.0 User Guide* for more information. | SNMP trap server |

*Table 1-8 Ports Used in Prime Access Registrar (continued)*

| Names | Description | Port Numbers | Service of the Ports | Access from Network Node | Configuration Setting | Protocol Name and Reference |
|---|---|---|---|---|---|---|
| CPAR SIGTRAN Stack (radius) | Listen on these ports for internal configuration from stack manager events | 9041/TCP | Stack Manager Configuration/Event Listener | This service can be accessed from local host by Prime Access Registrar – Radius Process. | N/A | CPAR Specific IPC Protocol implementation |
| | | 9041/UDP | Stack Manager Configuration/Event Listener | This service can be accessed from local host by Prime Access Registrar – Radius Process. | N/A | CPAR Specific IPC Protocol implementation |
| CPAR SIGTRAN stack manager(m3ua-stackmgr) | Configure stack and receive configuration from m3ua-cliclient | 9100/TCP | SIGTRAN Stack Manager | This service can be accessed from local host by Prime Access Registrar – Radius Process and m3ua-cliclient Process. | N/A | CPAR Specific IPC Protocol implementation |
| | | 9100/UDP | SIGTRAN Stack Manager | This service can be accessed from local host by Prime Access Registrar – Radius Process and m3ua-cliclient Process. | N/A | CPAR Specific IPC Protocol implementation |

1. If an error occurs while starting the Diameter SCTP interface, add **install sctp /bin/true** to /etc/modprobe.conf. Then, configure port 3868 with Type Diameter-TCP using aregcmd in /Radius/Advanced/Ports.

# Related Documentation

For a complete list of Cisco Prime Access Registrar documentation, see the *Cisco Prime Access Registrar 9.0 Documentation Overview*.

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

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

## Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.