

## Cisco Access Registrar 4.2

### General Questions

**Q. What is Cisco® Access Registrar?**

**A.** Cisco Access Registrar is a RADIUS server that is designed to meet the specific needs of service providers, including deployment, performance, scalability, resilience, and extensibility requirements.

**Q. What is new for Cisco Access Registrar 4.2?**

**A.** Cisco Access Registrar 4.2 is a minor release with some enhancements and bug fixes that will benefit a number of current and potential customers. The primary features of Release 4.2 include dynamic service authorization, session scalability (up to 4 million sessions/server), Lightweight Directory Access Protocol (LDAP) bind-based authentication, update to the Oracle client library and server, certificate management with Certificate Revocation List (CRL),] shared secret hiding, WiMAX support, support of T series Sun servers, and server virtualization support among many other features.

**Q. What are the benefits of Cisco Access Registrar?**

**A.** Cisco Access Registrar delivers a full-featured, customizable RADIUS server so that service providers can focus on delivering revenue-generating services. The latest release, Cisco Access Registrar 4.2, provides functionality to deliver the latest authentication, authorization, and accounting (AAA) server technology for broadband and mobile wireless networks, wireless LANs, and public wireless LANs.

**Q. How widely is Cisco Access Registrar deployed?**

**A.** Cisco Access Registrar is a mature, carrier-class RADIUS server that has been deployed worldwide by numerous large enterprises and service providers, both large and small, since 1998.

### Technical Questions

**Q. What hardware specification should I use?**

**A.** This depends on the request rate. It is possible to support hundreds or thousands of requests per second with a single server, although a second server is typically purchased for redundancy. Where multiple Cisco Access Registrar servers are deployed, each Cisco Access Registrar server may be a primary RADIUS server for a set of network access servers (NASs) and a backup for others. For examples of hardware specifications, please see the Cisco Access Registrar 4.2 Release Notes.

**Q. What, if any, additional software is needed to use Cisco Access Registrar?**

**A.** Apart from a fully patched and supported version of the operating system, Cisco Access Registrar is self-contained. It has a fast, built-in database that stores the server configuration and user information. No extra software is required to enforce user or group session limits, allocate IP addresses from IP pools defined in Cisco Access Registrar, configure Cisco Access Registrar to act as a RADIUS proxy, or to use the configuration replication feature.

**Note:** A graphical user interface (GUI) is available for Cisco Access Registrar; to enable the GUI, the server should have JRE 1.4.x installed.

**Q. Is Cisco Access Registrar compatible with equipment from other vendors?**

**A.** Yes. Cisco maintains compatibility with the latest RADIUS standards to help ensure that Cisco Access Registrar is interoperable with any RADIUS-compliant client, regardless of vendor. In addition, Cisco Access Registrar's attribute dictionary comes predefined with the attributes of many third-party vendors. Cisco Access Registrar's dictionary of extensible new attributes can be added at any time.

**Q. Is Cisco Access Registrar scalable?**

**A.** Directory and database capabilities allow Cisco Access Registrar to support authentication and authorization for millions of users. Multiple Cisco Access Registrar servers can reference a distributed directory or database. Additionally, Cisco Access Registrar supports replication of its internal database to allow multiple servers to be similarly configured. Cisco Access Registrar's multithreaded architecture provides performance that scales with additional CPUs. Together, these features allow Cisco Access Registrar to scale to support large service deployments with high call rates.

**Q. What protocols, ports, or secure transmission methods are used between client (NAS) and Cisco Access Registrar server?**

**A.** For administration, TCP ports 2785 and 2786 are used. These ports are not configurable. The administrator password is never sent across the wire in clear text.

The Simple Network Management Protocol (SNMP) daemon provided with Access Registrar uses standard SNMP ports.

For RADIUS request processing, the network interfaces and ports used are configurable. By default, Cisco Access Registrar listens on ports 1645 and 1646, on all interfaces.

**Q. What are the basic components in Cisco Access Registrar and how are they implemented?**

**A.** Cisco Access Registrar basically consists of UNIX daemons and a very fast internal database. The internal database stores the AAA configuration and can also be used for storing user profiles.

Basically Cisco Access Registrar consists of three functional units:

- **Policy Engine:** A robust and extensible method of imposing per packet policies
- **AAA server:** A Radius server designed from the ground up for performance, scalability, and extensibility for deployment in complex service provider environments
- **Session Manager:** Keeps track of active user sessions and allows real-time query from external applications; allocates resources such as IP address per user, per group session limiting, and other methods.

**Q. What standards are supported by Cisco Access Registrar?**

**A.** Cisco Access Registrar supports the following RFCs:

- [2865](#) RADIUS
- [2866](#) RADIUS Accounting
- [2867](#) RADIUS Accounting Modifications for Tunnel Protocol Support

- [2868](#) RADIUS Attributes for Tunnel Protocol Support
- [3576](#) Dynamic Authorization Extensions (updates RFC2869, Packet of Disconnect [PoD] support only)
- [3579](#) RADIUS Support for Extensible Authentication Protocol (EAP) (updates RFC 2869)
- [2618](#) RADIUS Authentication Client MIB
- [2619](#) RADIUS Authentication Server MIB
- [2620](#) RADIUS Accounting Client MIB
- [2621](#) RADIUS Accounting Server MIB
- [4186](#) Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)

Cisco Access Registrar supports the following drafts/documents:

- Digest Authentication over RADIUS (draft-sterman-aaa-sip-00.txt)
- EAP-SIM draft 11 (draft-haverinen-pppext-eap-sim-11.txt)
- WiMAX support as per the Network Working Group (NWG) version 1.1.0 of the stage III document (WiMAX Forum)

**Q. Can Cisco Access Registrar process RADIUS requests differently based on attributes in the request?**

- A.** Yes. Cisco Access Registrar can be configured to dynamically decide how to process requests based on any attribute in the packet, including, but not limited to, username prefix or suffix, dialed number, or calling number. An access request can be processed using information in an LDAP directory server or an Oracle or MySQL database, forwarded to another RADIUS server, or handled through a combination of these methods. An accounting request can be processed locally into a file, forwarded to another RADIUS server, written to a database, or processed using a combination of these methods.

**Q. Can Cisco Access Registrar be configured to modify attributes in a RADIUS packet?**

- A.** In addition to the authorization process, in which attributes stored in Cisco Access Registrar's internal database or external database are returned in an access-accept packet, Cisco Access Registrar allows attributes in a RADIUS request, response, or proxy packet to be added, modified, or deleted.

**Q. Is Cisco Access Registrar able to reject an authentication request on the basis of RADIUS attributes other than the user credentials?**

- A.** Cisco Access Registrar supports the concept of check items. Check items are a list of Radius attribute value pairs that are associated with user groups or individual user profiles. On successful completion of legacy authentication, Access Register verifies the attributes in the check item list with those in the requests, and the values should match for successful response.

**Q. What are Cisco Access Registrar extensions?**

- A.** Cisco Access Registrar provides a number of extension points where customers or system integrators may extend the logic of the product through C/C++ shared libraries, Java, or Tool Command Language (TCL) scripts. These extension points allow access to incoming and outgoing RADIUS packets for complete processing control. Extension points also support the integration of completely proprietary AAA services with a RADIUS front end.

**Q. What session management features does Cisco Access Registrar have?**

- A.** Cisco Access Registrar is able to track user sessions. By tracking these sessions, Cisco Access Registrar can enforce session limits on a per user or group basis. It can also manage shared resources, including IP addresses, home-agent assignment, and on-demand address pools (for Multiprotocol Label Switching [MPLS] VPNs).

Cisco Access Registrar maintains an in-memory table of active user sessions. It can be configured to store RADIUS attributes in the session table. Cisco Access Registrar allows applications on the network to query this session table using either RADIUS or Extensible Markup Language (XML) queries from the 4.1 release.

Cisco Access Registrar can query sessions by their age, then release them and generate a PoD if necessary.

Session management can take place, independently, on each Cisco Access Registrar in the network, or one Cisco Access Registrar server can be designated to perform this function for the other Cisco Access Registrar servers in the network to provide centralized session management.

**Q. How much memory does Cisco Access Registrar's session management require?**

- A.** Each session can use up to a maximum of 8 Kilo Bytes (KB.) Normally it is much less than this.

Memory consumption will vary based on the number and types of resource managers used, by whether session notes are used, and by the number of sessions. Sessions are stored in one or more hash tables, so the size of the table grows linearly with the number of sessions. A customer reported that roughly 1 KB of memory per session was consumed for 4 million sessions. Session information is also stored on disk. A comparable amount of disk space is therefore also required during session management.

**Q. What types of accounting and billing systems does Cisco Access Registrar support?**

- A.** Cisco Access Registrar supports local flat-file accounting records, proxy RADIUS accounting, or writing records directly to an Oracle or MySQL database. In addition, Cisco Access Registrar can be configured to use a combination of these accounting methods when processing an accounting request.

These methods also allow either offline transfers or direct feeds of accounting records into a billing server.

Cisco Access Registrar provides a special billing interface, allowing billing vendors to integrate their systems into Cisco Access Registrar for prepaid functionality.

**Q. Does Cisco Access Registrar support Dynamic Host Configuration Protocol (DHCP) for IP address allocation?**

- A.** No, Cisco Access Registrar does not support DHCP for IP address allocations.

Instead, it is possible to define IP pools within Cisco Access Registrar for allocation.

It may be possible to create a custom service in Cisco Access Registrar to do IP allocation through DHCP.

**Q. Does Cisco Access Registrar come with an LDAP directory server?**

**A.** No, Cisco Access Registrar does not provide an LDAP directory server.

Cisco Access Registrar has been tested with the Sun ONE Directory Server and Novell eDirectory. OpenLDAP provides an open source LDAP directory.

**Q. Does Cisco Access Registrar support postpaid and prepaid subscriptions?**

**A.** Cisco Access Registrar supports both prepaid and postpaid subscriptions.

For postpaid, Cisco Access Registrar is very loosely coupled with billing systems:

(1) Cisco Access Registrar can proxy RADIUS accounting messages to billing systems directly, and (2) Cisco Access Registrar writes into a local file/ODBC database and the billing system reads from this.

When it comes to prepaid Cisco Access Registrar is more tightly interfaced with billing systems. Cisco Access Registrar supports Cisco real-time billing and the industry standard IS-835c prepaid standards.

**Q. Does Cisco Access Registrar support EAP authentication methods?**

**A.** EAP methods supported by Cisco Access Registrar are:

- EAP-SIM
- EAP-TLS
- EAP-TTLS
- EAP-MSChapV2
- EAP-MD5
- EAP-LEAP
- EAP-GTC,
- Protected EAP

**Q. How is redundancy achieved in Cisco Access Registrar?**

**A.** Cisco Access Registrar supports replication allowing configurations in a master server to replicate multiple slave servers. This allows easy deployment of redundant architecture with the ease of maintaining a cluster of servers with identical configuration and centralized management.

**Q. What information does the Cisco Access Register server log?**

**A.** Cisco Access Registrar server maintains a comprehensive list of log files to record server statistics and user information. All the logs are stored locally in the UNIX file system as text files and allow easy deployment of tools that parse the log files. The files can be exported through file transfer.

Cisco Access Registrar maintains the following logs:

- **Server log:** Logs server statistics such as reloads
- **Command log:** Logs administrator commands through the command-line interface (CLI) and GUI
- **RADIUS log:** Logs RADIUS traffic information on the server, including successful and unsuccessful authentications with the reason for rejection, and so on

- **RADIUS traces:** The verbosity of this log can be set from the CLI and GUI. At maximum verbosity, it logs packet traces of each request and response, the internal services that processed the packet, and the extension point scripts, if any, that were applied on the flow.

**Q. Does Cisco Access Registrar output any messages to help in troubleshooting?**

- A.** Yes, Cisco Access Registrar has extensive logging. All the log files are in the logs directory of the Cisco Access Registrar installation. To get detailed troubleshooting output, turn on tracing by entering the following command in the aregcmd command-line interface utility:

```
trace /r 5
```

This will generate detailed server processing information to the logs/name RADIUS 1 trace file.

**Q. How do I configure Cisco Access Registrar?**

- A.** You use the command-line interface utility, aregcmd. It stores the configuration information in the internal database.

**Q. Is this offering supported by the Cisco Technical Assistance Center (TAC)?**

- A.** Yes, the Cisco TAC, worldwide, has received Cisco Access Registrar training and provides 24-hour support.

**Q. What data imports and exports does this offering support? How is this achieved?**

- A.** Cisco Access Registrar's configuration is stored in an embedded database. Cisco Access Registrar ships with backup and restore utilities (mcdshadow and keybuild, respectively) for this database.

To configure Cisco Access Registrar from another data source, Cisco Access Registrar commands have to be generated. These can be placed in a file and executed in one go. RADIUS accounting records are stored in flat text files for import into external databases.

**Q. How does Cisco Access Registrar decide to mark a remote server as down or offline?**

- A.** Cisco Access Registrar marks a remote server as down when it does not receive a response from it. It makes use of three properties in the RemoteServer object:
- MaxTries
  - InitialTimeout
  - ReactivateTimerInterval

Cisco Access Registrar waits InitialTimeout millisecond (ms) for a response from the remote server. If it does not receive a response, it resends the request up to MaxTries times, doubling the previous timeout each time. If it has not received a response after MaxTries and it has not received responses from any other requests sent to the same remote server during the same period, it marks that server as down.

Checking whether it has received responses to other requests sent to the same remote server allows for the situation where the remote server is responding to some requests but not all and, therefore, is not down.

Cisco Access Registrar will wait ReactivateTimerInterval ms before marking the remote server as up again. Cisco Access Registrar will mark all remote servers as up after a reload.

**Q. How do you use return attributes in Access-Accept?**

- A.** For users stored in Cisco Access Registrar 3.0 and later, each user object has an Attributes subobject in which return attributes can be entered:

```
[ //localhost/Radius/UserLists/Default/bob ]
Name = bob
Description =
Password =
AllowNullPassword = FALSE
Enabled = TRUE
Group~ =
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
Attributes/
    Session-Timeout = 600
CheckItems/
```

The profile object may be used to define attributes to be used by many users. The profile object is defined once and then applied to each user that requires it.

For users stored in an LDAP directory or Oracle database, values may be stored in the user record and then mapped to the RADIUS attributes to be returned to the user. This mapping is done in the RemoteServer object.

**Q. How do you add the new vendor-specific attributes (VSAs)?**

- A.** Cisco Access Registrar has the extensibility to add new VSAs on the fly and it can be added under:

```
[ //localhost/Radius/Advanced/Attribute\ Dictionary/Vendor-
Specific/Vendors/]
```

To add any VSA:

```
[ //localhost/Radius/Advanced/Attribute Dictionary/Vendor-
Specific/Vendors]
Add Cisco
Cd Cisco
Name = Cisco
Description =
VendorID = 9
Type = SUB_ATTRIBUTES
VendorTypeSize = 8-bit
HasSubAttributeLengthField = TRUE
SubAttribute Dictionary/
Cd SubAttribute Dictionary
SubAttribute Dictionary/
Add Cisco-AVPair
Cisco-AVPair/
Name = Cisco-AVPair
Description =
SubAttribute = 1
Type = STRING
```

Min = 0  
Max = 253

Customers can add their VSAs similar to the preceding one.

**Q. How do you know which version of Cisco Access Registrar is running?**

**A.** You can use `pkginfo -l CSCoar` or, in `aregcmd`, check the Version property in the RADIUS object:

```
--> ls /Radius
```

**Q. What protocols, ports, or secure transmission are used between client and server?**

**A.** For administration, TCP ports 2785 and 2786 are used. These ports are not configurable. The administrator password is never sent across the wire in clear text.

The SNMP daemon provided with Cisco Access Registrar uses standard SNMP ports.

For RADIUS request processing, the network interfaces and ports used are configurable. By default, Cisco Access Registrar listens on ports 1645 and 1646, on all interfaces.

**Q. How is the health number in aregcmd calculated in Cisco Access Registrar?**

**A.** The number starts off at 10, indicating a “healthy” server.

The following things decrement the server's health:

- The rejection of an access request
- Configuration errors
- Running out of memory
- Errors reading from the network
- Dropping packets that cannot be read (because the server ran out of memory)
- Errors writing to the network

As you can see, if there are a few access rejects, it can bring down the server health. In production servers, the health value will usually be somewhere between 3 and 10 depending on the number of access rejects.

**Q. Is there any way to get Cisco Access Registrar to log successful authentications?**

**A.** Yes. By default, `/Radius/Advanced/LogServerActivity` is set to false.

This means that Cisco Access Registrar will only log rejected and dropped authentications to the name `_radius_1_log` log file. To log successful authentications as well, set its value to true.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)