



## Release Notes for Cisco Access Registrar, 4.0

---

Cisco Access Registrar (AR) 4.0 provides RADIUS authentication, authorization, and accounting (AAA) services for service providers and enterprises. Cisco AR supports service provider deployment of access services by centralizing AAA information and simplifying provisioning and management.

Cisco AR is a standards-based Remote Authentication Dial-in User Service (RADIUS) and proxy RADIUS server designed for high-performance, extensibility, and integration with external data stores and systems.

Cisco AR supports a range of access technologies from traditional dial and broadband to wireless LANs and mobile wireless. Cisco AR supports the latest wireless authentication protocols such as Extensible Authentication Protocol and Protected EAP used in wireless LAN deployments. Cisco AR also is able to make real-time AAA requests to billing systems to support prepaid applications.



### Note

---

Cisco AR 4.0 can be used with Solaris 8, Solaris 9, or the Red Hat 7.3 Linux operating system using kernel version 2.4.20-24.7 (or later), glibc version 2.2.5-42 (or later).

---

**CCO Date: April 2005**  
**Revised: March 18, 2008**



### Note

---

Cisco AR 4.0 uses a different licensing mechanism than the license key used in releases prior to Cisco AR 3.5. Before you upgrade your Cisco AR server to Cisco AR 4.0.1 software, you must install a license file. Refer to [Cisco AR 4.0 Licensing](#) for detailed information about Cisco AR 4.0.1 licensing and how to install the license file.

---

## Contents

This release note contains the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 4](#)
- [Related Documentation, page 6](#)
- [Cisco AR 4.0 Licensing, page 6](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© <year> Cisco Systems, Inc. All rights reserved.

- [Installing Cisco AR on Solaris, page 9](#)
- [Installing Cisco AR on Linux, page 14](#)
- [Preparing to Use SNMP, page 18](#)
- [Cisco AR Performance, page 18](#)
- [Caveats, page 21](#)

## Introduction

Cisco Access Registrar (AR) is a fast, highly available and extensible RADIUS platform that provides intelligent Authentication, Authorization and Accounting (AAA) services across all subscriber access technologies. Cisco AR 4.0 has been designed for Service Providers who demand a carrier-class AAA server with great performance and extensibility.

This section lists and describes the new features and enhancements in Cisco AR 4.0. Cisco AR 4.0.1 provides the following new features in addition to those features in Cisco AR 3.5.

## EAP-FAST

Cisco AR supports the EAP-FAST authentication method. EAP-FAST uses the EAP-MSChapV2 method for credential provisioning and EAP-GTC for authentication. Credential provisioning typically occurs only during the client's initial EAP-FAST authentication. Subsequent authentications rely on the provisioned credential and will usually omit the provisioning step.

EAP-FAST is an authentication protocol designed to address the performance shortcomings of prior TLS-based EAP methods while retaining features such as identity privacy and support for password-based protocols. The EAP-FAST protocol is described by the IETF draft *draft-cam-winget-eap-fast-01.txt* (draft version 1).

The EAP-FAST credential is known as a Protected Access Credential (PAC) and contains information used to secure the authentication operations. Parts of the PAC are encrypted by the server and are not visible to other entities. Clients are expected to securely store PACs locally for use during authentication.

Configuring EAP-FAST involves creating and configuring the required EAP-MSChapV2 and EAP-GTC services as well as the EAP-FAST service with the appropriate parameters.

You can use the **radclient** test tool to confirm that the EAP services are properly configured and operational.

## EAP-SIM

Cisco AR 4.0 supports EAP-SIM version 16. In a GSM network a subscriber is issued a *smart card* called the subscriber identity module (SIM) that contains a secret key (Ki) and an International Mobile Subscriber Identity (IMSI). The key (Ki) is also stored in the GSM authentication center located with the Home Location Registry (HLR).

An access point uses the Cisco AR RADIUS server to perform EAP-SIM authentication of mobile clients. Cisco AR must obtain authentication information from the HLR. Cisco AR contacts the MAP gateway that performs the MAP protocol over SS7 to the HLR.

## Graphical User Interface (GUI)

Cisco AR 4.0 provides a limited-function GUI that supports many of the every day configuration requirements of the Cisco AR system administrator.

## RADIUS Query

Cisco AR 4.0 supports a new service type called radius-query that can be used to query cached data through Radius packets. This radius-query service contains a list of session managers to be queried from and a list of (cached) attributes to be returned in the Access-Accept packet in response to a Radius Query request. Cisco AR 4.0 also supports caching and querying of multi-valued attributes.

The Radius Query service should be selected through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service. The reason for this is that the Radius Query request comes in as an Access-Request and the server has no way of knowing whether it is a Radius Query request or normal authentication request. Setting the Query-Service environment variable tells the Cisco AR server that the request is a Radius Query request so the Cisco AR server can process the request with the radius-query service set in the Query-Service environment variable.

When a Radius Query service is selected to process an Access-Request, it queries the configured list of Session Managers for a matching record using the QueryKey value configured in the session-cache Resource Manager referenced under these Session Managers as key. If a matching record is found, an Access-Accept containing a list of cached attributes present (based on the configuration) in the matched record is sent back to the client. If the session cache contains a multi-valued attribute, all values of that attribute are returned in the response as a multi-valued attribute. If there is no matching record, an Access-Reject packet is sent to the client.

Cisco AR 4.0 introduces scripting points at the Session Manager level along with application programming interfaces (APIs) to access cached information present in the session record. You can use these scripting points and APIs to write extension point scripts to modify the cached information.

## Change of Authorization

Cisco AR 4.0 provides a Change of Authorization (CoA) feature, also known as *hot-lining*, that enables a system administrator to send CoA packets to a client device whenever a user needs to be hot-lined. The trigger as to when a CoA should be sent to hot-line a user depends on site specific policies. Changes to the **query-session** command through the Cisco AR CLI and GUI provide the CoA functionality. A system administrator can issue the **query-session** command through a script or an application whenever there is a need to trigger hot-lining for a user.

## Windows Domain Authentication

The domain-auth Remote Server is used with the Windows Domain Authentication feature. Cisco AR Cisco AR 4.0 supports user authentication and authorization using an Active Directory (AD) database residing on a Windows 2000 server. Authentication against AD is enabled by the CiscoSecure Remote Agent (CSRA), which must be installed on a Windows server, a Domain Controller (DC), or on the server hosting the AD database.

**Note**

---

You can download the CiscoSecure Remote Agent from <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des>. The file to download is **Remote-Agent-ACSse-win-v3.3.2.2-K9.zip**, described as Remote Agent for Windows for Solution Engine, 3.3.2.2, dated 28-OCT-2004.

---

During authentication, the user credentials are sent to the CSRA, which authenticates the credentials with the WDC/AD. The user optionally can specify the domain name along with their UserID when they log in. If the domain is not specified, authentication is first performed with the local WDC/AD (default domain as specified in the remote server configuration), then with all the other trusted domain controllers, one by one until the user is found in any of the trusted WDC/ADs.

This *failover* to other domains is taken care by the local (default) WDC/AD. The local WDC/AD maintains a list of trusted domains and when the user is not found in the local AD, the WDC queries the trusted WDC/ADs, to see if any one those had the user in it. If any of the WDC/ADs has the user, those credentials would be used to authenticate the user.

The WDC/AD authentication stops at the first *hit* and does not check other domains even if the user credentials do not match (resulting in an authentication failure). When a domain is specified, authentication is performed only on that domain. This domain should be either the local WDC/AD or one of the trusted WDC/ADs.

A 128-bit Blowfish (variant) encryption algorithm secures the communication between the Cisco AR and CSRA. The session key for this encryption is negotiated when the connection is established. Establishing the communication tunnel between the Cisco AR and CSRA is performed transparently and does not have to be configured in Cisco AR.

## IP Range and Wildcard Support

Cisco AR has been modified to support grouping of client configuration objects by enhancing the Client IPAddress property and adding a new NetMask property. The Client IPAddress property has been enhanced to allow for specification of a set of IP addresses using their range or with a like wildcard character.

When a range is configured for the Client's IPAddress property, any incoming requests whose source address belongs to the range specified, will be allowed for further processing by the server. Similarly when a wildcard (an asterisk '\*' in this case) is specified, any incoming requests whose source address matches the wildcard specification will be allowed. In both the cases, the configured client properties like SharedSecret, and Vendor are used to process the requests.

## System Requirements

This section describes the system requirements for installing the Cisco AR software.

**Note**

---

Before installing Cisco AR 4.0 software, ensure that your server's operating system software is up to date and that all recommended patches have been installed. Note the need for a Solaris 8 patch described in [Solaris 8 Patch Requirement, page 6](#).

---

## Full Installation

Table 1 lists the system requirements for a full installation of Cisco AR.

**Table 1** Full Installation Requirements

Component	Requirement
CPU Architecture	SPARC
OS Version	Solaris 8, Solaris 9, or Linux
Minimum RAM	256 MB
Recommended RAM	512 MB
Recommended Disk Space	175 MB

## Client-Only Installation

Table 2 lists the system requirements for installing the client-only component of Cisco AR.

**Table 2** Client-Only Requirements

Component	Requirement
CPU Architecture	SPARC
OS Version	Solaris 8 or Solaris 9
Minimum RAM	32 MB
Recommended RAM	64 MB
Recommended Disk Space	120 MB



### Note

The client-only installation is available only when using the Solaris operating system.

The recommended disk space does not include the amount of space needed for accounting records which can grow rapidly depending on how frequently you process and remove them from the Cisco AR disk. If Cisco AR runs out of disk space, it could cause the loss of accounting information and the corruption of session management information.

## Co-Existence With Other Network Management Applications

To achieve optimal performance, Cisco Access Registrar should be the only application running on a single machine. You can choose to run collaborative servers such as an Oracle or SQL database system, an LDAP server, or another Solaris application. There are no known conflicts with any other Solaris applications.

You can configure Cisco AR to avoid UDP port conflicts with other network management applications. The most common conflicts occur when other applications also use ports 2785 and 2786. Another possible conflict could be SNMP. If you configure and use SNMP on your Cisco AR server, no another application can be configured to use SNMP on the Cisco AR machine.

**Note**

---

Cisco Network Registrar and Cisco AR cannot co-exist on the same workstation.

---

## Solaris 8 Patch Requirement

Cisco AR 4.0 uses OpenSSL software to generate certificates for 'https' communication. OpenSSL software uses Solaris internal devices `/dev/urandom` and `/dev/random` devices while generating certificates, but these devices are not in Solaris 8.

You can add `/dev/urandom` and `/dev/random` devices to Solaris 8 by installing patch 112438 (sparc) available at the following URL:

<http://sunsolve.sun.com>

**Note**

---

If you attempt to install the Cisco AR 4.0.x package in Solaris 8 without this patch, Cisco AR reports an error.

---

## Related Documentation

The following is a list of the documentation for Cisco Access Registrar 4.0.1. You can access the URLs listed for each document at [www.cisco.com](http://www.cisco.com) on the World Wide Web. Cisco recommends that you refer to the documentation in the following order:

*Cisco Access Registrar 4.0 Documentation Guide* (78-16709-01)

[http://www.cisco.com/en/US/docs/net\\_mgmt/access\\_registrar/4.0/roadmap/docgd.html](http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/4.0/roadmap/docgd.html)

*Cisco Access Registrar 4.0 Installation and Configuration Guide* (OL-6544-01)

[http://www.cisco.com/en/US/docs/net\\_mgmt/access\\_registrar/4.0/installation/guide/incfg.html](http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/4.0/installation/guide/incfg.html)

*Cisco Access Registrar 4.0 User's Guide* (OL-6543-01)

[http://www.cisco.com/en/US/docs/net\\_mgmt/access\\_registrar/4.0/user/guide/user.html](http://www.cisco.com/en/US/docs/net_mgmt/access_registrar/4.0/user/guide/user.html)

## Cisco AR 4.0 Licensing

Cisco AR 4.0 uses a licensing mechanism that enables you to activate different features in Cisco AR using a combination of different license keys. During system initialization, the Cisco AR server sets up the licensing data model and activates any features that are properly licensed.

## Licensed Features

Table 3 lists the names of the features that require licenses. As new licensed features are added to Cisco AR, new license files will also be required.

**Table 3** Cisco AR 4.0 Licensed Features

Feature Name	Description
AR-STANDARD	Standard Cisco AR feature set including EAP-FAST and Windows Domain Authentication
AR-HLR	HLR Proxy feature for EAP-SIM service <b>Note</b> Cisco AR 4.0 supports EAP-SIM draft v16.
AR-PREPAID	Prepaid Billing feature for Prepaid service
AR-CACHE	Identity Caching and RADIUS Query features
AR-CPU	Standard Cisco AR feature set for Cisco AR servers with multiprocessors

## Getting Cisco AR 4.0 Feature Licenses

When you order the Cisco AR 4.0 product, a text license file will be sent to you in EMail. If you are evaluating the software, Cisco will provide you with an evaluation license.

If you decide to upgrade your Cisco AR software and add a feature, a new text license file will be sent to you in EMail when you order the upgrade.

If you receive a Software License Claim Certificate, you can get your Cisco AR license file at one of the two following URLs:

- [www.cisco.com/go/license](http://www.cisco.com/go/license)

Use this site if you are a registered user of Cisco Connection Online.

- [www.cisco.com/go/license/public](http://www.cisco.com/go/license/public)

Use this site if you are not a registered user of Cisco Connection Online.

Within one hour of registration at either of the above web sites, you will receive your license key file and installation instructions in email.

## Installing Cisco AR 4.0 Licenses

You must have a license in a directory on the Cisco AR machine before you attempt to install Cisco AR software. If you have not installed the Cisco AR license file before beginning the software installation, the installation process will fail.

You can store the Cisco AR license file in any directory on the Cisco AR machine. During the installation process, you will be asked the location of the license file, and the installation process will copy the license file to the `/opt/CSCOar/license` directory, or `$INSTALL/license` if you are not using the default installation location.

The license file might have the name `ciscoar.lic`, but it can be any filename with the suffix `.lic`. To install the Cisco AR license file, you can copy and paste the text into a file, or you can simply save the file you receive in EMail to an accessible directory.

## Upgrading Your Cisco AR 4.0 License File

If you add additional features that require licenses, you can open the file in `/opt/CSCOar/license` and add additional lines to the license file, or you can create an additional license file to hold the new lines. If you add a new file, remember to give it a `.lic` suffix.

If you upgrade your Cisco AR license for additional features, you must restart the Cisco AR server for the new license to take effect. To restart the Cisco AR server, enter the following on the server command line:

```
/opt/CSCOar/bin/arserver restart
```

## Sample License File

The following is an example of a Cisco AR 4.0 license file.

```
INCREMENT AR-STANDARD cisco 4.0 27-apr-2005 uncounted HOSTID=ANY \
  NOTICE="<LicFileID></LicFileID><LicLineID></LicLineID> \
  <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
INCREMENT AR-CACHE cisco 4.0 27-apr-2005 uncounted HOSTID=ANY \
  NOTICE="<LicFileID></LicFileID><LicLineID></LicLineID> \
  <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
INCREMENT AR-PREPAID cisco 4.0 27-apr-2005 uncounted HOSTID=ANY \
  NOTICE="<LicFileID></LicFileID><LicLineID></LicLineID> \
  <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
INCREMENT AR-HLR cisco 4.0 27-apr-2005 uncounted HOSTID=ANY \
  NOTICE="<LicFileID></LicFileID><LicLineID></LicLineID> \
  <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
INCREMENT AR-CPU cisco 4.0 27-apr-2005 uncounted HOSTID=ANY \
  NOTICE="<LicFileID></LicFileID><LicLineID></LicLineID> \
  <PAK>dummyPak</PAK>" SIGN=ABCDEF123456
```

## Displaying License Information

Cisco AR provides two ways of getting license information using `aregcmd`:

- `aregcmd` command-line option
- Launching `aregcmd`

### aregcmd Command-Line Option

Cisco AR provides a new `-l` command-line option to `aregcmd`. The syntax is:

```
aregcmd -l directory_name
```

where `directory_name` is the directory where the Cisco AR license file is stored. The following is an example of the `aregcmd -l` command:

**aregcmd -l /opt/CSCOar/license**

Licensed Application: Cisco Access Registrar (Standard Version)

Following are the licensed components:

	NAME	VERSION	EXPIRY_INFO
	====	=====	=====
	AR-Standard	4.0	27-Apr-2005
	AR-Prepaid	4.0	27-Apr-2005
	AR-HLR	4.0	27-Apr-2005
	AR-Cache	4.0	27-Apr-2005
	AR-CPU	4.0	27-Apr-2005

## Launching aregcmd

The Cisco AR server displays license information when you launch **aregcmd**, as shown in the following:

**aregcmd**

```
Cisco Access Registrar 4.0.0.3 Configuration Utility
Copyright (C) 1995-2004 by Cisco Systems, Inc. All rights reserved.
Cluster:
User: admin
Password:
Logging in to localhost

[ //localhost ]
  LicenseInfo = AR-Standard 4.0 (expires on 27-Apr-2005)
                AR-Prepaid 4.0 (expires on 27-Apr-2005)
                AR-HLR 4.0 (expires on 27-Apr-2005)
                AR-Cache 4.0 (expires on 27-Apr-2005)
                AR-CPU 4.0 (expires on 27-Apr-2005)

  Radius/
  Administrators/

Server 'Radius' is Running, its health is 10 out of 10
```

## Installing Cisco AR on Solaris

This section describes the software installation process when installing Cisco AR software on a Solaris workstation for the first time.

**Note**


---

Cisco AR 4.0 can be used with Solaris 8 or Solaris 9.

---

This section includes the following subsections:

- [Deciding Where to Install](#)
- [Installing Cisco AR Software from CD-ROM](#)
- [Installing Downloaded Software](#)
- [Common Solaris Installation Steps](#)

**Tips**

Before you begin to install the software, check your workstation's `/etc/group` file and make sure that group *staff* exists. The software installation will fail if group *staff* does not exist before you begin.

## Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for Cisco AR 4.0 software is `/opt/CSCOar`. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

## Installing Cisco AR Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the Cisco AR 4.0 CD-ROM. If you are installing downloaded software, proceed to [Installing Downloaded Software](#).

- 
- Step 1** Place the Cisco AR software CD-ROM in the Cisco AR workstation CD-ROM drive.
- Step 2** Log in to the Cisco AR workstation as a root user, and enter the following command line for Solaris 8:
- ```
pkgadd -d /cdrom/cdrom0/kit/solaris-2.8 CSCOar
```
- or the following for Solaris 9:
- ```
pkgadd -d /cdrom/cdrom0/kit/solaris-2.9 CSCOar
```
- Step 3** Proceed to [Common Solaris Installation Steps](#).
- 

## Installing Downloaded Software

This section describes how to uncompress and extract downloaded Cisco AR 4.0 software and begin the software installation.

- 
- Step 1** Log in to the Cisco AR workstation as a root user.
- Step 2** Change directory to the location where you have stored the uncompressed tarfile.
- ```
cd /tmp
```
- Step 3** Use the following command line to uncompress the tarfile and extract the installation package files.
- ```
zcat CSCOar-4.0.1-sol8-k9.tar.gz | tar xf -
```

**Note**

These instructions are for the Solaris 8 package. There is no difference in download or installation procedures for Solaris 8 or Solaris 9 other than the package name.

**Step 4** Enter the following command to begin the installation:

```
pkgadd -d /tmp CSCOar
```

where */tmp* is the temporary directory where you stored and uncompressed the installation files.

**Step 5** Proceed to [Common Solaris Installation Steps](#).

---

## Common Solaris Installation Steps

This section describes the installation process immediately after you have issued the **pkgadd** command installing from CD-ROM or from downloaded software.

```
Processing package instance <CSCOar> from </tmp>
```

```
Cisco Access Registrar 4.0.1 [SunOS-5.8, official]
(sparc) 4.0.1
```

```
Copyright (C) 1998-2005 by Cisco Systems, Inc.
```

```
This program contains proprietary and confidential information.
```

```
All rights reserved except as may be permitted by prior written consent.
```

```
This package contains the Access Registrar Server and the
Access Registrar Configuration Utility. You can choose to
perform either a Full installation or just install the
Configuration Utility.
```

```
What type of installation: Full, Config only [Full] [?,q]
```

**Step 6** For a full install, press **Enter**.

```
Where do you want to install <CSCOar>? [/opt/CSCOar] [?,q]
```

**Step 7** Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

```
Access Registrar requires FLEXlm license file to operate. A list
of space delimited license files or directories can be supplied as
input; license files must have the extension ".lic".
```

```
Where are the FLEXlm license files located? [] [?,q]
```

**Step 8** Enter the directory where you have stored the Cisco AR 4.0 license file.

```
Access Registrar provides a Web GUI. It requires J2RE version
1.4.* to be installed on the server.
```

```
If you already have a compatible version J2RE installed, please
enter the directory where it is installed. If you do not, the
compatible J2RE version can be downloaded from:
```

```
http://java.sun.com/
```

```
Where is the J2RE installed? [?,q] /nfs/insbu-cnstools/java
```

The J2RE is required to use the Cisco AR GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.

**Note**


---

If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

---

**Step 9** Enter the directory or mount point where the J2RE is installed.

If you are not using ORACLE, press Enter/Return to skip this step.  
 ORACLE installation directory is required for ODBC configuration.  
 ORACLE\_HOME variable will be set in /etc/init.d/arsserver script

Where is ORACLE installed? [] [?,q]

**Step 10** If you plan to use Oracle accounting, enter the location where you have installed Oracle; otherwise press **Enter**.

If you want to learn about Access Registrar by following the examples in the Installation and Configuration Guide, you need to populate the database with the example configuration.

Do you want to install the example configuration now [n] [y,n,?,q]

**Step 11** When prompted whether to install the example configuration now, reply **Y** or **N** to continue.

You can add the example configuration at any time by running the command:

```
/opt/CSCOAr/bin/aregcmd -f /opt/CSCOAr/examples/cli/add-example-configuration.rc
```

**Note**


---

You can delete the example configuration at any time by running the command  
**/opt/CSCOAr/usrbin/aregcmd -f /opt/CSCOAr/examples/cli/delete-example-configuration.rc.**

---

The selected base directory </opt/CSCOAr> must exist before installation is attempted.

Do you want this directory created now [y,n,?,q] y

**Step 12** Enter **Y** to enable the installation process to create the **/opt/CSCOAr** directory.

```
## Executing checkinstall script.
Using </opt/CSCOAr> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
```

The following files are being installed with setuid and/or setgid permissions:

```
/opt/CSCOAr/.system/screen <setuid root>
/opt/CSCOAr/bin/aregcmd <setgid staff>
/opt/CSCOAr/bin/radclient <setgid staff>
```

Do you want to install these as setuid/setgid files [y,n,?,q]

**Step 13** Enter **Y** to install the **setuid/setgid** files.

This package contains scripts which will be executed with super-user permission during the process of installing this package.

Do you want to continue with the installation of <CSCOAr> [y,n,?]

**Step 14** Enter **Y** to continue with the software installation.

No further interaction is required; the installation process should complete successfully and the **arservagt** is automatically started.

```

Installing Cisco Access Registrar 4.0.1 [SunOS-5.8, official] as <CSCOar>

## Installing part 1 of 1.
/opt/CSCOar/.system/add-example-config
/opt/CSCOar/.system/run-ar-scripts
/opt/CSCOar/.system/screen
/opt/CSCOar/README
/opt/CSCOar/bin/arbug
/opt/CSCOar/bin/nasmonitor
/opt/CSCOar/bin/share-access
/opt/CSCOar/bin/xtail
/opt/CSCOar/java/javadoc.tar.gz
.
.
inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/jndi-resources-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/manager-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/proxy-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/README.txt
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/realm-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/RUNNING.txt
  inflating:
/opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/security-manager-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/ssl-howto.html
  creating: /opt/CSCOar/jakarta-tomcat-4.0.6/work/
# setting up product configuration file /opt/CSCOar/conf/car.conf
# linking /etc/init.d/arserver to /etc/rc.d files
# removing old session information
# flushing old replication archive
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Thu Apr 14 14:12:02
2005
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Thu Apr 14 14:12:02
2005

We will now generate an RSA key-pair and self-signed certificate that
may be used for test purposes
Generating a 1536 bit RSA private key
.....++++
.....++++
writing new private key to '/cisco-ar/certs/tomcat/server-key.pem'
-----
Server self-signed certificate now resides in /cisco-ar/certs/tomcat/server-cert.pem
Server private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem

Remember to install additional CA certificates for client verification
unable to write 'random state'
Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent...tail: cannot open input
completed.
The Radius server is now running.
# done with postinstall.

Installation of <CSCOar> was successful
hostname root /tmp##

```

## Configuring SNMP

If you choose not to use the SNMP features of Cisco AR, the installation process is completed. To use SNMP features, complete the configuration procedure described in [Preparing to Use SNMP, page 18](#).

## RPC Bind Services

The Cisco AR server and the **aregcmd** CLI requires RPC services to be running before the server is started. If the RPC services are stopped, you must restart rpc services, then restart the Cisco AR server. Use the following commands to restart RPC services:

```
/opt/CSCOar/bin/arserver stop
```

```
/etc/init.d/rpc start
```

```
/opt/CSCOar/bin/arserver start
```

If RPC services are not running, the following message is displayed when you attempt to start aregcmd:

```
Login to aregcmd fails with the message:
400 Login failed
```

# Installing Cisco AR on Linux

This section describes the software installation process when installing Cisco AR 4.0 software on a Linux workstation for the first time.



### Note

Cisco AR 4.0 can be used with the Red Hat 7.3 Linux operating system using kernel version 2.4.20-24.7 (or later), glibc version 2.2.5-42 (or later).

This section includes the following subsections:

- [Deciding Where to Install](#)
- [Installing Cisco AR Software from CD-ROM](#)
- [Common Linux Installation Steps](#)



### Tips

Before you begin to install the software, check your workstation's **/etc/group** file and make sure that group *staff* exists. The software installation will fail if group *staff* does not exist before you begin.

## Deciding Where to Install

Before you begin the software installation, you should decide where you want to install the new software. The default installation directory for Cisco AR 4.0 software is **/opt/CSCOar**. You can use the default installation directory, or you can choose to install the Cisco AR software in a different directory.

## Installing Cisco AR Software from CD-ROM

The following steps describe how to begin the software installation process when installing software from the Cisco AR 4.0 CD-ROM. If you are installing downloaded software, proceed to [Installing Downloaded Software](#).

- Step 1** Place the Cisco AR 4.0 software CD-ROM in the Cisco AR workstation CD-ROM drive.
- Step 2** Log in to the Cisco AR workstation as a root user and find a temporary directory, such as **/tmp**, to store the Linux installation file.



**Note** The temporary directory requires at least 70 MB of free space.

- Step 3** Change directory to the CD-ROM.
- ```
cd /cdrom/cdrom0/kit/linux-2.4
```
- Step 4** Copy the **CSCOAr-4.0.1-lnx24-install-k9.sh** file to the temporary directory.
- ```
cp CSCOAr-4.0.1-lnx24-install-k9.sh /tmp
```
- Step 5** Change the permissions of the **CSCOAr-4.0.1-lnx24-install-k9.sh** file to make it executable.

```
chmod 777 CSCOAr-4.0.1-lnx24-install-k9.sh
```

To continue the installation, proceed to [Common Linux Installation Steps](#).

## Common Linux Installation Steps

This section describes how to install the downloaded Cisco AR 4.0 software for Linux and begin the software installation.



**Note** The Cisco AR Linux installation automatically installs **aregcmd** and **radclient** as setgid programs in group **adm**.

- Step 1** Log in to the Cisco AR workstation as a root user.
- Step 2** Change directory to the location where you have stored the **CSCOAr-4.0.1-lnx24-install-k9.sh** file.

```
cd /tmp
```

- Step 3** Enter the name of the script file to begin the installation:

```
CSCOAr-4.0.1-lnx24-install-k9.sh
```

```
Name          : CSCOAr                      Relocations: /opt/CSCOAr
Version       : 4.0.1                       Vendor: Cisco Systems, Inc.
Release      : 1112362579                   Build Date: Fri Apr 1 06:46:30 2005
Install date: (not installed)               Build Host: sentret.cnslab.cisco.com
Summary      : Access Registrar, a carrier-class RADIUS server
build_tag: [Linux-2.4.20, official]
```

Copyright (C) 1998-2005 by Cisco Systems, Inc.  
 This program contains proprietary and confidential information.  
 All rights reserved except as may be permitted by prior written consent.

This package contains the Access Registrar Server and the Access Registrar Configuration Utility. All the Client, Server, and Configuration utilities will be installed.

Where do you want to install <CSCOar> [/opt/CSCOar] [?,q]

**Step 4** Press **Enter** to accept the default location of **/opt/CSCOar**, or enter a different directory to be used as the base installation directory.

Access Registrar requires FLEXlm license file to operate. A list of space delimited license files or directories can be supplied as input; license files must have the extension ".lic".

Where are the FLEXlm license files located? [/opt/CSCOar/license] [?,q]

**Step 5** Enter the directory where you have stored the Cisco AR 4.0 license file.

Access Registrar provides a Web GUI. It requires J2RE version 1.4.\* to be installed on the server.

If you already have a compatible version of J2RE installed, please enter the directory where it is installed. If you do not, the compatible J2RE version can be downloaded from:

<http://java.sun.com/>

Where is the J2RE installed? [] [?,q]

The J2RE is required to use the Cisco AR GUI. If you already have a Java 2 platform installed, enter the directory where it is installed.



**Note** If you do not provide the J2RE path, or if the path is empty or unsupported, the installation process exits.

If you are not using ORACLE, press Enter/Return to skip this step. ORACLE installation directory is required for ODBC configuration. ORACLE\_HOME variable will be set in /etc/init.d/arserver script

Where is ORACLE installed? [] [?,q]

**Step 6** Enter the location where you have installed Oracle, otherwise press **Enter**.

If you want to learn about Access Registrar by following the examples in the Installation and Configuration Guide, you need to populate the database with the example configuration.

Do you want to install the example configuration now? [n]: [y,n,?,q] y

**Step 7** When prompted whether to install the example configuration now, reply **Y** or **N** to continue.



**Note** You can delete the example configuration at any time by running the command **/opt/CSCOar/usrbin/aregcmd -f /opt/CSCOar/examples/cli/delete-example-configuration.rc**.

```
unpack the rpm file done
Preparing... ##### [100%]
```

```

1:CSCOarui-add          ##### [100%]
Archive:  ./jakarta-tomcat-4.0.6.zip
  creating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/bootstrap.jar
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/bin/catalina.bat
.
.
.
inflating:
/opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/security-manager-howto.html
  inflating: /opt/CSCOar/jakarta-tomcat-4.0.6/webapps/tomcat-docs/ssl-howto.html
  creating: /opt/CSCOar/jakarta-tomcat-4.0.6/work/
Preparing...          ##### [100%]
1:CSCOar              ##### [100%]
relink arserver
# flushing old replication archive
# creating initial configuration database
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" started Thu Apr 14 11:51:29
2005
Rollforward recovery using "/opt/CSCOar/data/db/vista.tjf" finished Thu Apr 14 11:51:29
2005

# add-example-config y
JAVA_ROOT /nfs/insbu-cnstools/java-linux
JAVA_HOME /nfs/insbu-cnstools/java-linux
# setting ORACLE_HOME and JAVA_HOME variable in arserver
ORACLE_HOME
JAVA_HOME /nfs/insbu-cnstools/java-linux
set JAVA_HOME
calling gen-tomcat
/cisco-ar/certs/tomcat/server-cert.pem exists, no action taken.
unable to write 'random state'

```

**Note**


---

The message unable to write 'random state' does not indicate an error and should be ignored.

---

```

Tomcat private RSA key now resides in /cisco-ar/certs/tomcat/server-key.pem
Starting Access Registrar Server Agent..completed.
The Radius server is now running.

```

```
hostname root /tmp###
```

## Configuring SNMP

If you choose not to use the SNMP features of Cisco Access Registrar, the installation process is completed. To use SNMP features, complete the configuration procedure described in [Preparing to Use SNMP](#), page 18.

## Preparing to Use SNMP

If you plan to use the SNMP features of Cisco Access Registrar, complete the following steps:

- 
- Step 1** Become root user by entering **su**, then the root password.
- Step 2** Enter the following commands to disable the Sun SNMP daemon and allow Cisco AR's SNMP daemon to function:
- ```
/etc/rc3.d/S76snmpdx stop
/etc/rc3.d/S77dmi stop
```
- Step 3** Enter the following commands to prevent the Sun SNMP daemon from restarting after a reboot by entering the following:
- ```
mkdir /etc/rc3.d/.disabled
mv /etc/rc3.d/S76snmpdx /etc/rc3.d/.disabled
mv /etc/rc3.d/S77dmi /etc/rc3.d/.disabled
```

## Cisco AR Performance

This section lists the primary performance test results. Although the hardware and operating system used for performance testing of AR 4.0 are identical to those used for performance testing of AR 3.5, the performance numbers are not directly comparable to the previously published performance numbers for AR 3.5 due to various configuration differences of the testbed. Performance regression testing of AR 3.5 on the identical testbed as used for AR 4.0 testing has shown that the performance of AR 4.0 is very close to AR 3.5 in most cases (within the margin of error of less than 3% difference). Some specific tests for Session Manager scenarios show improved performance for AR 4.0. A separate document providing comparative performance numbers for AR 3.5 and 4.0 will be available through Cisco AR product marketing in the near future.

As applies for all benchmark testing, the ultimate determination of suitability of a particular hardware and software combination can only be made by running performance tests in a real-world operational environment. The performance numbers that follow provide only guidelines for the performance that can be expected from AR 4.0.

The tests cases were run on a Sun Fire V210 with 2GB RAM, 2x1000MHz UltraSPARC-3i processors, 36GB SCSI-UW disk, and Solaris 8 64-bit kernel. The reported numbers are an average of 100 test runs.

The LDAP servers run on an HP Kayak XU with 256MB RAM, 2x500MHz Pentium 3 processors, 9.1GB SCSI-UW disk, and Windows 2000 Service Pack 4. No special performance tuning was made to the servers or to Cisco AR. All LDAP tests ran with three proxy servers in round robin. The Oracle servers run on the same platform and number of servers in round robin.

The LDAP vendor is the iPlanet Directory Server 4.11. The Oracle server version is 9.2.0.1. Both data stores have 10,000 users.

The Oracle accounting tests were run using Sun Fire v210 and a Sun V480 (with Oracle 9.2 database).

Numbers are given in RADIUS Pairs Per Second (RPPS). In general, one transaction is one RADIUS request/response pair (access-request and access-accept). The following is the specific pair usage for each test type:

- One AA transaction uses one RADIUS pair
- One AAA transaction uses three RADIUS pairs

- One accounting only transaction uses two RADIUS pairs

Table 4 lists performance results for a local database.

**Table 4 Performance of Local Database**

Test	Results
AA	2221 RPPS
AAA	2067 RPPS
Accounting only	2564 RPPS
AA with Session Management	837 RPPS
AAA with Session Management	948 RPPS
AA Latency	1.40 ms
Accounting Latency	130.21 ms
AA with Session Management Latency	125.94 ms

Table 5 lists performance results of Cisco AR with a proxy server with a local database.

**Table 5 Performance of Proxy Server with Local Database**

Test	Results
AA	2065 RPPS
AAA	1728 RPPS
Accounting only	1860 RPPS
AA with Session Management	789 RPPS
AAA with Session Management	939 RPPS
AA Latency	3.96 ms
Accounting Latency	106.96 ms
AA with Session Management Latency	151.15 ms

Table 6 lists performance results of Cisco AR using an LDAP server.

**Table 6 Performance of LDAP Server**

Test	Results
AA	979 RPPS
AAA	2295 RPPS
AA with Session Management	360 RPPS
AAA with Session Management	1020 RPPS

Table 7 lists performance results of Cisco AR using ODBC with local accounting.

**Table 7** Performance of ODBC with Local Accounting

Test	Results
AA	1246 RPPS
AAA	2070 RPPS
AA with Session Management	700 RPPS
AAA with Session Management	993 RPPS

Table 8 lists performance results of Cisco AR using ODBC with Oracle accounting.

**Table 8** Performance of ODBC with Oracle Accounting

Test	Results
AA	883 RPPS
AAA	1263 RPPS
Accounting only	1354 RPPS
AA with Session Management	695 RPPS
AAA with Session Management	807 RPPS

Table 9 lists performance results of Cisco AR using EAP-SIM authentication. EAP-SIM performance to a large degree depends on the EAP-SIM protocol implementation on the client side and the performance of the back-end SIM authentication infrastructure (such as the HLR/AuC, signaling network). The performance numbers that follow give an indication of what can be achieved with a synthetic test client and a TCL script simulating the back-end infrastructure. Real-world server performance might be faster if you use real SIM authentication hardware.

**Note**

An authentication sequence for authentication and authorization requires three request-challenge-accept pairs. An authentication sequence for authentication, authorization, and accounting requires five request-challenge-accept pairs.

**Table 9** Performance of Cisco AR Using EAP-SIM

Test	Authentications/second	RPPS
AA	365	1095
AAA	263	1315
AA with Session Management	200	600
AAA with Session Management	270	1350

# Caveats

This section provides information about known anomalies in Cisco AR 4.0 and anomalies (from previous versions of Cisco AR) that have been fixed in Cisco AR 4.0.1.

## Known Anomalies in Cisco AR 4.0.1

Table 10 lists known anomalies in Cisco AR 4.0.1 and other anomalies that might still be active from previous releases of Cisco AR.

**Table 10** Known Anomalies in Cisco AR 4.0.1

Bug	Description
CSCdw74227	<p>Increasing the maximum number of file descriptors in <code>/etc/system</code> causes <b>aregcmd</b> to stop working</p> <p>Symptom: <b>aregcmd</b> cannot login to the server, even on a fresh install.</p> <p>Conditions: The has raised the maximum number of file descriptors in <code>/etc/system</code> to increase the maximum number of open file handles.</p> <p>Workaround: Remove the maximum number of file descriptors lines and reboot the Cisco AR server.</p>
CSCdz57329	<p>LDAP server loses some parameters after concurrent <b>ckitem save</b> operations</p> <p>Symptom: After a configuration save, some of the LDAP server configuration parameters are lost.</p> <p>Conditions: This might occur when LDAP to Check Item mappings are saved in two concurrent <b>aregcmd</b> sessions.</p> <p>Workaround: Do no edit LDAP to Check Item mappings in concurrent <b>aregcmd</b> sessions.</p>
CSCeb46418	<p>Misleading <b>aregcmd</b> error when swap space consumed</p> <p>Symptom: <b>aregcmd</b> indicates that it was unable to read the internal configuration.</p> <p>Conditions: This might occur when all swap space on a machine is in use.</p> <p>Workaround: Redistribute applications so there is adequate swap space on the machine.</p>
CSCeb86676	<p>Error message for malformed packet wrong with LDAP.</p> <p>Symptom: Trace messages indicate that poorly-formatted packets were rejected due to unknown user names or incorrect passwords.</p> <p>Conditions: This might occur when LDAP is used for authentication or authorization.</p> <p>Workaround: In some cases, it may be necessary to turn trace levels up and examine the contents of packets. Generally this will not be required.</p>
CSCec11705	<p>An error message for ODBC and FDS is confusing</p> <p>Symptom: ODBC is configured properly, but the following message appears in the log:</p> <pre>/opt/CSCOar/logs/name_radius_1_log:08/22/2003 9:35:29 name/radius/1 Error Server 0 ODBC client (Connection 30): SQLConnect failed: IM002 [unixODBC][Driver Manager]Data source name not found, and no default driver specified</pre> <p>Conditions: This might occur when the number of open file descriptors exceeds the system limit.</p> <p>Workaround: Increase the number of open file descriptors permitted, or ignore the message when it occurs.</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCec53453	<p>Parse errors appear in Replication messages</p> <p>Symptom: The message <code>parse failed \&lt;unknown user\&gt;</code> appears in the log.</p> <p>Conditions: This might occur with replication configured.</p> <p>Workaround: Ignore these messages; the server should recover without intervention.</p>
CSCec56101	<p>After lock manager killed, all servers die</p> <p>Symptom: After the lock manager is killed, all other servers die.</p> <p>Conditions: This might occur if the lock manager is manually killed on busy multi-processor machines.</p> <p>Workaround: None</p>
CSCed03397	<p>USR VSAs have incorrect format</p> <p>Symptom: 3Com PDSN complains about the USR VSAs being returned to it from AR</p> <p>Conditions: Cisco AR is configured to use USR VSAs. Cisco AR uses the normal VSA format of:</p> <p style="padding-left: 40px;">type, length, vendor, vendor type, length, data</p> <p>instead of the USR format:</p> <p style="padding-left: 40px;">type, length, vendor, vendor type, data</p> <p>Workaround: Use an extension point script to configure the USR VSAs.</p>
CSCed12389	<p>Attribute Text-Ascend-Data-Filter found in configurations upgraded to 3.5.1</p> <p>Symptom: The attribute Text-Ascend-Data-Filter is present in configurations upgraded to AR 3.5 from previous versions.</p> <p>Conditions: An upgrade to Cisco AR 3.5 from a previous version of Cisco AR is done.</p> <p>Workaround: None.</p>
CSCed61132	<p>Down server, <b>reload</b> after deletion times out and no deletion occurs</p> <p>Symptom: After a session using dynamic DNS ends, the reverse zone mappings are never deleted from the zone.</p> <p>Conditions: This might occur if the DNS server is unreachable when the session ends, and the Radius server is reloaded or restarted before the DNS server is available again.</p> <p>Workaround: Manually delete the names from the zone.</p>
CSCed77005	<p>Response-Type not read at ServiceOutgoing</p> <p>Symptom: Cisco AR ignores the Response-Type environment variable at the service outgoing scripting point.</p> <p>Conditions: An LDAP service was in use for authentication and authorization. An outgoing script on this service checked if the request was rejected. If it was, the script changed the Response-Type to Access-Accept.</p> <p>Workaround: If the same script is placed at the server outgoing scripting point, the script successfully accepts the user.</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCed82514	<p>Remote server statistics are displayed for POD-enabled clients</p> <p>Symptom: The <b>stats</b> command displays remote server statistics for POD-enabled clients.</p> <p>Conditions: Clients with POD-enabled exist in the configuration.</p> <p>Workaround: None.</p>
CSCed83041	<p>After load of large user file with replication, packets are dropped</p> <p>Symptom: The master replication server ceases responding to packets after a very large number of users are loaded.</p> <p>Conditions: This might occur with very large numbers of users and probably also with large numbers of profiles.</p> <p>Workaround: Load larger user files into both master and member servers prior to starting up replication, or load in large files during very off-peak problems when a backup server is available.</p>
CSCed88582	<p>Some <b>trace</b> messages need to be updated</p> <p>Symptom: Some <b>trace</b> messages that are displayed during creation and sending of disconnect-requests are inaccurate.</p> <p>Conditions: Disconnect-requests are created and sent to clients.</p> <p>Workaround: None.</p>
CSCee70452	<p><b>aregcmd</b> asks to save when no changes have been made</p> <p>Symptom: <b>aregcmd</b> asks to save when no changes made.</p> <p>Conditions: After login, the looked at a client object, but did not change anything. On exit, <b>aregcmd</b> asks if the wishes to save changes.</p> <p>Workaround: None</p>
CSCee88854	<p>The <b>unset 0</b> command causes decrement of entry index in indexed lists</p> <p>Symptom: The <b>unset 0</b> command causes the entry indices in indexed lists to be decremented by one, and <b>aregcmd</b> segmentation faults on subsequent commands with valid indices.</p> <p>Conditions: The <b>unset</b> command is used with index 0.</p> <p>Workaround: Use the <b>unset</b> command with valid indices only.</p>
CSCee90401	<p><b>aregcmd</b> does not show configuration when the Radius server crashes continuously</p> <p>Symptom: <b>aregcmd</b> does not show the configuration and displays the following:</p> <pre>Unable to obtain a valid license from server.  Check license file configuration and restart server.  [ //localhost ]   LicenseInfo =   Administrators/</pre> <p>Conditions: This occurs when radius process reloads by itself continuously.</p> <p>Workaround: None</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCef07321	<p>Query-sessions with-Age with only units succeeds</p> <p>Symptom: The <b>query-sessions</b> command succeeds when only units are specified with the with-Age option.</p> <p>Conditions: The <b>query-sessions</b> command is invoked with only units specified with the with-Age option.</p> <p>Workaround: None.</p>
CSCef07329	<p>No disconnect-NAK sent if proxied POD times out</p> <p>Symptom: Cisco AR does not send a disconnect-NAK to the remote server if the disconnect-request forwarded to a client from the remote server times out.</p> <p>Conditions: A disconnect-request forwarded to a client from a remote server times out.</p> <p>Workaround: None.</p>
CSCef09629	<p>With stress, Cisco AR proxy shows SignatureMismatch errors</p> <p>Symptom: In RADIUS proxy client, some responses were dropped due to Signature mismatch.</p> <p>Conditions: Occurs when RADIUS proxy server is placed under heavy load.</p> <p>Workaround: None</p>
CSCef16872	<p>With MultipleServersPolicy of RoundRobin, more packets accepted</p> <p>Symptom: An ODBC accounting server accepts packets sent during traffic bursts, even though its remote server is down.</p> <p>Conditions: This might occur if the MultipleServersPolicy configuration parameter is set to RoundRobin.</p> <p>Workaround: Set the MultipleServersPolicy configuration parameter to Failover.</p>
CSCef34090	<p>File descriptor count not consistent across Cisco AR server reloads</p> <p>Symptom: Radius process file descriptor count not consistent</p> <p>Conditions: Occurs after executing <b>aregcmd reload, stop, and start</b>.</p> <p>Workaround: None</p>
CSCef34635	<p>Problems with BADTIME log message</p> <p>Symptom: A message appears in the log that a DNS update has been rejected due to BADTIME. This message states that the DNS and DHCP server times are identical.</p> <p>Conditions: This might occur when updates are rejected due to time skews between the DNS and Radius systems. Note that the times are given in GMT format.</p> <p>Workaround: Ignore the message which indicates that the times match. Use tracing to view the DNS Update message itself, which will indicate the time skew between the two machines.</p>
CSCef54940	<p>In Linux, Cisco AR starts in port 1812, but all port defaults show 1645</p> <p>Symptom: <b>aregcmd</b> assumes default port values of 1645 and 1646</p> <p>Conditions: When <b>Radius/Services</b> configuration specifies a radius port value, Radius server takes it as default and listens there. But <b>aregcmd</b> will still show 1645 and 1646 as the default ports.</p> <p>Workaround: None</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCef61137	<p><b>aregcmd</b> synchronization error message</p> <p>Symptom: In a second <b>aregcmd</b> session, the following message appears during a <b>save</b>:</p> <pre>Synchronizing with external changes to database... done. 500 Internal Error Synchronizing with external changes to database failed</pre> <p>Conditions: Two <b>aregcmd</b> commands sessions are editing the same object.</p> <p>Workaround: Enter <b>save</b> again, and the error message will not appear.</p>
CSCef63044	<p>Radius crashes if wrong feature line given in separate file</p> <p>Symptom: Radius server crashes when an invalid prepaid feature line with a wrong value is specified in a separate license file.</p> <p>Conditions: An invalid prepaid feature line with a wrong value is specified in a separate license file</p> <p>Workaround: Specify valid feature lines in all license files.</p>
CSCef70457	<p>With HTTP digest, Reply-Message not sent when UserPasswordInvalid</p> <p>Symptom: Reply-Message not present in Access-Reject</p> <p>Conditions: With HTTP digest authentication and local-users service, send an Access-Request with digest response generated from invalid password.</p> <p>Workaround: None</p>
CSCef80124	<p>Cisco AR cores when using ODBC accounting and reloading while packets sent</p> <p>Symptom: Cores occur when ODBC accounting is in use and the server is reloaded.</p> <p>Conditions: This might occur when the ODBC remote server is configured so that there will be insertion errors, and the server is under stress.</p> <p>Workaround: The core occurs during a <b>reload</b> and has minimal operational impact, but we recommend you configure ODBC accounting servers in accordance with the database tables which are available.</p>
CSCef83845	<p>CHAP request without CHAP-Challenge attribute not cached properly</p> <p>Symptoms: Trusted ID implicit authentication requests are failing when using CHAP.</p> <p>Conditions: The identity was cached using a CHAP request that did not contain the CHAP-Challenge attribute. The implicit authentication request might or might not contain the CHAP-Challenge attribute.</p> <p>Workaround: Always send the CHAP-Challenge attribute in the explicit authentication request or only use PAP.</p>
CSCef86758	<p>The <b>aregcmd save</b> and <b>reload</b> commands generate a crash with myodbc</p> <p>Symptom: Cisco AR server restarted by itself, when <b>save</b> and <b>reload</b> commands are issued consecutively after adding a MYODBC remoteserver.</p> <p>Conditions: Occurs after adding a MYODBC remote server and executing <b>save</b> and <b>reload</b> commands consecutively.</p> <p>Workaround: None</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCef86899	<p>In Linux, Java vendor outgoing script occasionally causes crash</p> <p>Symptom: Cisco AR server cores on Linux when a Java extension script is executed at the Vendor outgoing script point.</p> <p>Conditions: This problem does not occur on Solaris and only occurs on Linux when the <b>java_extnpoints</b> script is run immediately after the <b>java_methods</b> script. Also, scripts set at all scripting points other than the Vendor outgoing scripting point work fine.</p> <p>Workaround: If possible, use another extension script point or another scripting language.</p>
CSCef90638	<p>Cisco AR log files need to check log size at startup and roll if needed</p> <p>Symptom: The <b>aregcmd</b> log does not roll when it gets to the configured rolling size.</p> <p>Conditions: The <b>aregcmd</b> log grows to a size that is larger than the LogFileSize property, but it does not roll.</p> <p>Workaround: An <b>aregcmd</b> session must have 25 commands after reaching the roll size before the log will roll.</p>
CSCef95743	<p>OutagePolicy not effective with http-digest and ODBC</p> <p>Symptom: http-digest request is rejected</p> <p>Conditions: OutagePolicy is set to AcceptAll with http-digest and with ODBCDatastore</p> <p>Workaround: None</p>
CSCef96916	<p>When Algorithm is other than md5, md5sess, or http-digest, Cisco AR server accepts the user</p> <p>Symptom: User is accepted when a http-digest request is sent with Algorithm value other than MD5/MD5-sess.</p> <p>Conditions: Sending an http-digest request with unknown Algorithm value.</p> <p>Workaround: None</p>
CSCef97167	<p>Changing MySQL server name does not reflect after Cisco AR server reload</p> <p>Symptom: For some requests, Cisco AR server uses the previously configured MySQL server name.</p> <p>Conditions: Modifying the MySQL server name in ODBCDataSources and doing a <b>reload</b>.</p> <p>Workaround: Perform a complete restart of the Cisco AR server.</p>
CSCeg12829	<p>When using Internet Explorer for the Cisco AR GUI, the Back button returns you to old or incorrect values</p> <p>Symptom: Web GUI displays old values in an edit form.</p> <p>Conditions: A change is submitted with a syntax error. The operator presses the Back to return to the edit form.</p> <p>Workaround: When the edit form is re-displayed, it displays the current values in the database. You must re-enter all changes.</p>
CSCeg36153	<p>Number of entries in radiusAccServerTable is less than actual</p> <p>Symptom: With SNMP, number of radiusAccServerTable entries are less than actual.</p> <p>Conditions: Enabling SNMP and querying for radiusAccServerTable entries of RADIUS-ACC-CLIENT-MIB.</p> <p>Workaround: None</p>

**Table 10** Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeg45085	<p>OutagePolicy for accounting request does not work as documented</p> <p>Symptom: When OutagePolicy set to RejectAll and accounting service is unavailable, accounting requests does not perform Session Management.</p> <p>Conditions: RemoteServers configured under the accounting service are unreachable and Service OutagePolicy is set to RejectAll.</p> <p>Workaround: None</p>
CSCeg48805	<p>Some RemoteServers statistics counters occasionally show negative values</p> <p>Symptom: Statistics output of Remoteserver totalRequestsPending and totalRequestsOutstanding occasionally display negative values.</p> <p>Conditions: This might occur when Cisco AR is receiving high load of packets and sending to remote server.</p> <p>Workaround: None</p>
CSCeh04514	<p>When deleting something that was already deleted, back is odd</p> <p>Symptom: When trying to edit data fields in the GUI at the same time as another administrator, the GUI might give an error message and clear all data fields.</p> <p>Conditions: When two administrators are editing the same data in the GUI and one attempts to edit an object that the other has already deleted, one administrator will receive an error message and a link to return to the original record. When the administrator follows the link, all data fields in the object are cleared.</p> <p>Workaround: Do not simultaneously edit and delete the same object from two different GUI windows.</p>
CSCeh15106	<p>Intermittent java.lang.ClassCastException</p> <p>Symptom: Cisco AR GUI throws a Java ClassCastException when editing some EAP-FAST or PEAP settings.</p> <p>Conditions: The GUI (or rather the Java VM used by the GUI) throws a Java ClassCastException in one of the servlets used to edit fields for an EAP method. This error occurs intermittently and rarely when changing the inner service or some service settings of a tunneled EAP service (for example, EAP-FAST or PEAP).</p> <p>The same type of GUI error might also be triggered after service settings are changed from a CLI and the updated values are displayed by the GUI.</p> <p>Workaround: Repeat the edit operation and, if possible, change the entered values slightly.</p>
CSCeh38746	<p>Deleting sessions is not handled correctly in backing store</p> <p>Symptom: After a reload AR's knowledge of user sessions might contain user sessions that were released earlier before reload.</p> <p>Conditions: The disk partition on which the Cisco AR server is installed is full.</p> <p>Workaround: Make more space available on the partition. Cisco AR might need to be restarted.</p>
CSCeh40071	<p><b>aregcmd</b> log file does not roll in Linux machines</p> <p>Symptom: The server command logfile <b>aregcmd_log</b> does not roll over at the size specified by the LogFileSize property.</p> <p>Conditions: This happens frequently on Linux and occasionally on Solaris. Other log files, for example <b>config_mcd</b>, roll over properly, such as when a new log file is created when the indicated file size is reached.</p> <p>Workaround: It might help to change the LogFileSize property to a value slightly greater than the current log file size to allow another attempt at rollover. If the server command log grows too large, stop the server, manually and remove or back up the log file, then restart the server.</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeh41879	<p>View-only administrator can release sessions</p> <p>Symptom: View-only administrator can release sessions.</p> <p>Conditions: An administrator who logs in as a view-only administrator is able to release sessions from the session list page of the web GUI.</p> <p>Workaround: None other than to discourage view-only administrators from releasing sessions.</p>
CSCeh44351	<p>Deleted view-only administrator becomes full-administrator</p> <p>Symptom: A view-only administrator user logged into GUI temporarily acquires full administrator privileges if the administrator user's record is deleted.</p> <p>Conditions: A view-only administrator user is logged into the GUI and another, fully privileged administrator user deletes the view-only administrator's user record. For the duration of the current session, the view-only administrator is promoted to a fully privileged administrator with read and write permissions. Once the administrator logs out of the current session (or is automatically logged out after the idle timeout), the view-only administrator can no longer log in because the administrator user record no longer exists.</p> <p>Workaround: Do not delete user records for view-only administrators while they are logged in.</p>
CSCeh50552	<p>Validation does not catch Client IP 0.0.0.0 after adding an invalid configuration</p> <p>Symptom: After <b>aregcmd</b> detects some invalid client IP address settings, the server validation routine might not detect if the IP address is set to an invalid value (such as 0.0.0.0) for a second time.</p> <p>Conditions: When setting a RADIUS client IP address to an invalid value from the CLI, the validation routine might not detect if another invalid value is entered. This might happen especially if the first invalid value included a dash character used to specify a range and appeared to indicate an invalid address, such as 0.0.0-1.1.1.1.</p> <p>Workaround: Always enter a correct IP address value.</p>
CSCeh50799	<p>Java crashes: WebUI in use while java scripts test runs</p> <p>Symptom: An administrator is logged out of the Web configuration interface.</p> <p>Conditions: This might occur if Java services are modified while the Web configuration interface is in use.</p> <p>Workaround: Log into the Web user interface a second time.</p>
CSCeh54984	<p>Validation required when radius-query service is set to defaultAAA</p> <p>Symptom: No validation messages are printed when a service of type radius-query is used as the default authentication, authorization or accounting service.</p> <p>Conditions: This will occur when a service of type radius-query is used as the default authentication, authorization or accounting service.</p> <p>Workaround: Do not do this. The Radius-query service is invoked by setting the Query-Service environment variable.</p>
CSCeh55025	<p>Java Session APIs called outside of Session Manager restarts Radius</p> <p>Symptom: The Radius process crashes and is restarted by the server agent.</p> <p>Conditions: This can occur if a session-specific call is made by a Java extension at an extension point other than the session manager extension points.</p> <p>Workaround: Do not use session-specific APIs in Java extensions that will not be called from session management extension points.</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeh56666	<p>Missing XML tag in an XML request document should get processed</p> <p>Symptom: An XML query request of an ICE session cache manager is rejected by the server with the error message:</p> <pre>Rejecting XML Request: packet failed to parse</pre> <p>Conditions: A session cache resource manager is configured with QueryMappings to allow XML queries, for example of user name and IP address. When the server is queried for one of those values using an XML request that is missing the XML tag <code>&lt;?xml version="1.0"?&gt;</code>, the server will reject the query request due to the missing XML version tag.</p> <p>Workaround: Make sure XML requests always include a proper version tag.</p>
CSCeh57195	<p>Crashes referencing server statistics log</p> <p>Symptom: Web User Interface users are logged out after clicking on Server Stats Log.</p> <p>Conditions: This might occur at times when many configuration changes are taking place.</p> <p>Workaround: Log into the Web UI server again.</p>
CSCeh58158	<p>Reload hung on two machines after much UI use</p> <p>Symptom: The Cisco AR UI ceases to respond.</p> <p>Conditions: This might happen if many configuration operations are performed. The Radius server log will indicate that a <b>reload</b> is in process, but the <b>reload</b> never completes.</p> <p>Workaround: Restart the Cisco AR server.</p>
CSCeh58732	<p>Re-login does not create a new session</p> <p>Symptom: An administrator logs in to the GUI but appears to be logged in as the previous administrator.</p> <p>Conditions: An administrator logs in to the GUI as a view-only administrator, then returns to the login page and logs in as a read-write administrator without first logging out. The administrator remains logged in as the view-only administrator.</p> <p>Workaround: You must explicitly log out with the <b>logout</b> button before logging in as another administrator.</p>
CSCeh60774	<p>Online help does not mention a restart is required to disable or enable http or https protocols.</p> <p>Symptom: It is still possible to open an http or https Web user interface connection, even though this protocol has been disabled in the <b>server.xml</b> file.</p> <p>Conditions: This might occur when the <b>server.xml</b> file has been edited but the servers have not been restarted.</p> <p>Workaround: Use <b>arserver restart</b> to restart the servers after modifying the <b>server.xml</b> file.</p>
CSCeh61488	<p>Request-Type not set in remote server OutgoingScript</p> <p>Symptom: Request-Type environment variable always empty.</p> <p>Conditions: A script on a remote server's OutgoingScript is attempting to read the Request-Type environment variable.</p> <p>Workaround: If possible, try to use the server IncomingScript. Otherwise, there is no workaround.</p>

Table 10 Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeh61503	<p>Request-Type and Response-Type are the same for remote server IncomingScript</p> <p>Symptom: Request-Type and Response-Type environment variables always have the same result.</p> <p>Conditions: A script on a remote server's IncomingScript is attempting to read the Request-Type environment variable.</p> <p>Workaround: If possible, try to use the server OutgoingScript. Otherwise, there is no workaround.</p>
CSCeh61842	<p>Server reload might hang if Cisco Secure Remote Agent (CSRA) is not responding</p> <p>Symptom: The AAA server hangs while reloading. The last entry in the log file reads:</p> <pre>&lt;timestamp&gt; Log: Agent API: Attempting to connect to agent manager at &lt;IP address&gt;:2004</pre> <p>Conditions: This might occur if a remote server for Windows Domain Authentication (WDA) is configured and the CSRA is running on the remote server, but the remote server is not working properly (perhaps due to misconfiguration) or the CSRA is unable to complete the protocol for establishing the protected tunnel for WDA.</p> <p>If the local AAA server is reloaded while in this state (waiting for the establishment of the tunnel), the server process might hang and the server might have to be restarted.</p> <p>Note that if the AAA server is configured with an invalid WDA remote server address or the address of a remote server that is not running CSRA (including <b>localhost</b>), the attempt to connect to the CSRA will properly time out and server operation will not be affected (failure to connect CSRA will be logged).</p> <p>Workaround: Make sure the remote Windows server, including CSRA, is properly configured and responding to requests from the AAA server. Ensure the link to the remote server is stable and does not suffer from excessive packet delays or drops. If the local server is stuck after a reload, kill the server process using the <b>kill -9</b> command and restart the server. Reconfigure the server to use another remote server for WDA or disable it by pointing at a server not running CSRA (including <b>localhost</b>).</p>
CSCin45016	<p>Session Manager hangs while changing the system date</p> <p>Symptom: The <b>release-session</b> command of <b>aregcmd</b> hangs and also the RADIUS does not give response for access-requests and hangs in session management.</p> <p>Conditions: Occurs after changing the system date to an earlier time and not restarting the server.</p> <p>Workaround: Restart the Cisco AR server after changing the system date or time.</p>
CSCin46551	<p>Cisco AR server is reloaded when enabling SNMP and doing restart immediately thereafter.</p> <p>Symptom: RADIUS gets reloaded automatically.</p> <p>Conditions: Enabling SNMP in Cisco AR and restarting the server immediately.</p> <p>Workaround: None.</p>
CSCin53226	<p>On heavy load <b>odbc.ini</b> file becomes empty</p> <p>Symptom: The log reports that the ODBC datasource cannot be found.</p> <p>Conditions: This has only been observed with an extremely high number of ODBC data source connections and heavy load.</p> <p>Workaround: Replace the contents of the <b>/opt/CSCOar/odbc/etc/odbc.ini</b> file.</p>

**Table 10** Known Anomalies in Cisco AR 4.0.1 (continued)

Bug	Description
CSCin57842	LEAP challenge not sent when setting Response-Type to accept Symptom: User accepted without sending EAP challenge. Conditions: Setting the Response-Type to accept using rex or java script. Workaround: None
CSCin64112	With SNMP, occasionally <b>armedsvr</b> reloads itself Symptom: Occasionally <b>armedsvr</b> process is restarted automatically by Cisco AR server. Conditions: This might occur after enabling SNMP and restarting Cisco AR server. Workaround: None
CSCin64207	Upgrade fails when setting <b>ARIsCaseInSensitive</b> to false Symptom: Upgrade fails with the following error message 307 Object not found/Path ambiguous Conditions: <b>/Radius/Advanced/ARIsCaseInSensitive</b> flag is set to false. Workaround: Before upgrading, set <b>/Radius/Advanced/ARIsCaseInSensitive</b> to True. After upgrade revert the <b>/Radius/Advanced/ARIsCaseInSensitive</b> to false.

## Anomalies Fixed in Cisco AR 4.0.1

This section describes the anomalies known to exist in earlier versions of Cisco AR that have been fixed in Cisco AR 4.0.1.

**Table 11** Anomalies Fixed in Cisco AR 4.0.1

Bug	Description
CSCai02102	Session backing store can become corrupted if the disk partition becomes full Symptom: <b>aregcmd</b> fails while logging in or <b>aregcmd</b> fails while saving with an error message similar to "500 Internal Error / Checking to see if we needed to synchronize with external changes to database failed" or after a <b>reload</b> , Cisco AR's knowledge of user sessions is missing information that was present before the <b>reload</b> . Conditions: The disk partition upon which Cisco AR is installed is full. Workaround: Make more space available on the partition. You might need to restart Cisco AR.
CSCdw23443	Cisco AR <b>stats</b> command does not count packets dropped by outage policies Symptom: Some dropped packets are not counted by Cisco AR <b>stats</b> command. This is apparent when looking at the statistics from <b>aregcmd</b> or SNMP. Conditions: When packets are dropped by order of an outage policy. Workaround: None.

Table 11 Anomalies Fixed in Cisco AR 4.0.1 (continued)

Bug	Description
CSCdx43984	<p>AWACS should log messages when contents of cache are deleted</p> <p>Symptom: No messages logged when triplet cache entries are deleted.</p> <p>Conditions: Triplet caching is enabled and entries in the cache time out.</p> <p>Workaround: None.</p>
CSCdy51365	<p>Java services not hot-configured properly</p> <p>Symptom: Java services do not work until the server is reloaded.</p> <p>Conditions: A Java service is added and saved, and the server is not reloaded.</p> <p>Workaround: Reload the server on adding a Java service.</p>
CSCdy71586	<p>Class file not located if classpath set after java script configuration</p> <p>Symptom: The class file referenced by a Java extension script is not recognized if it is in a location other than the default classpath if the classpath is set to the class file location after the script is configured.</p> <p>Conditions: The classpath for Java extensions parameter is set after the Java extension script is configured.</p> <p>Workaround: Set the classpath for Java extensions before configuring the script or restart the server.</p>
CSCdz21344	<p>Concurrency control problem with user attributes</p> <p>Symptom: Attributes in a user's attributes or check-items directory are deleted in two different <b>aregcmd</b> sessions. Only one of the two attributes shows up as deleted in subsequent <b>aregcmd</b> sessions.</p> <p>Conditions: This only occurs when these attributes are deleted in two different <b>aregcmd</b> sessions.</p> <p>Workaround: Remove the attribute which was not deleted a second time.</p>
CSCdz57386	<p>Only one user present after concurrent <b>save</b>.</p> <p>Symptom: A created user is no longer visible.</p> <p>Conditions: This might occur when a new userlist is created, and a single new user is added to that list in two simultaneous <b>aregcmd</b> sessions.</p> <p>Workaround: Do not add new users to empty userlists in concurrent <b>aregcmd</b> sessions.</p>
CSCea18102	<p>Incorrect output when setting case sensitive flag</p> <p>Symptom: The output message is incorrect:</p> <p style="padding-left: 40px;"><b>set ""</b></p> <p>Conditions: The flag <b>/Radius/Advanced/ARisCaseInSensitive</b> has been set.</p> <p>Workaround: None.</p>



Table 11 Anomalies Fixed in Cisco AR 4.0.1 (continued)

Bug	Description
CSCed26188	<p>Incorrect error message when null attribute set under AttributesToBeCached</p> <p>Symptom: The error message displayed when a null attribute is set under AttributesToBeCached is incorrect.</p> <p>Conditions: A null attribute name is set under AttributesToBeCached.</p> <p>Workaround: None.</p>
CSCed28632	<p>Able to change Radius server name</p> <p>Symptom: The <b>save</b> command succeeds when the name of the Radius server is modified.</p> <p>Conditions: The name of the Radius server is modified.</p> <p>Workaround: None.</p>
CSCed55165	<p>Set port type to default value on port addition</p> <p>Symptom: Port type is set to null when a new port is added.</p> <p>Conditions: A new port is added.</p> <p>Workaround: None.</p>
CSCed65041	<p>The <b>stats</b> command always indicates no messages sent to prepaid server</p> <p>Symptom: The stats output always indicates that no messages have been sent to a prepaid server.</p> <p>Conditions: This will occur whenever a prepaid server is configured.</p> <p>Workaround: Ignore the output of the <b>stats</b> command for prepaid servers.</p>
CSCee36083	<p>EAP-nak iterates all services in the middle of authentication exchange</p> <p>Symptom: All services in the service list of an eap-negotiate service are iterated through again if an EAP-Nak is received in the middle of an authentication exchange.</p> <p>Conditions: An EAP-Nak is received when authentication using a specific EAP protocol has already commenced.</p> <p>Workaround: None.</p>
CSCee40054	<p>Unable to club -C switch of <b>aregcmd</b> with other switches</p> <p>Symptom: When the -C switch of <b>aregcmd</b> is clubbed with other switches, <b>aregcmd</b> prompts for the cluster.</p> <p>Conditions: The -C switch of <b>aregcmd</b> is clubbed with other switches.</p> <p>Workaround: Use the -C switch separately from other switches.</p>
CSCee92924	<p>No license or invalid license should show correct error message in command-line interface (CLI)</p> <p>Symptom: Invalid Default Authentication service error message displayed and Cisco AR stopped after a server reload.</p> <p>Conditions: Invalid or empty license file is available at <b>/opt/CSCOar/license</b> directory.</p> <p>Workaround: Copy the valid license file to the license directory.</p>
CSCee93258	<p>Cannot change value of enumerated attributes</p> <p>Symptom: After changing the value of an enumerated attribute, it is not possible to save the configuration.</p> <p>Conditions: This might occur when the value of an enumerated attribute is changed.</p> <p>Workaround: Use the <b>unset</b> command to delete the enumeration, then add it again.</p>

**Table 11** *Anomalies Fixed in Cisco AR 4.0.1 (continued)*

Bug	Description
CSCef06185	<p>The <b>aregcmd</b> gives a segmentation fault during validation in cache session</p> <p>Symptom: Setting the QueryKey to the wrong case in a session-cache identity resource manager will produce a segmentation fault during a <b>save</b>.</p> <p>Conditions: <b>aregcmd</b> segmentation fault while saving the configuration.</p> <p>Workaround: None</p>
CSCef09629	<p>With stress, Cisco AR proxy shows SignatureMismatch errors</p> <p>Symptom: In RADIUS proxy client, some responses were dropped due to Signature mismatch.</p> <p>Conditions: Occurs when RADIUS proxy server is placed under heavy load.</p> <p>Workaround: None</p>
CSCef10229	<p>XML request with format modifier in wrong case should be discarded</p> <p>Symptom: XML request document is processed when the format modifier in the &lt;Address&gt; tag is in capital format.</p> <p>Conditions: This occurs when the modifier attributes are in wrong case, and the XML request document is not discarded.</p> <p>Workaround: None</p>
CSCef15010	<p>Stale session not removed for accounting start</p> <p>Symptom: When querying for an identity, Cisco AR responds with the previous user on NAS IP and Port.</p> <p>Conditions: The previous user's accounting stop was lost or was not sent so the session manager did not remove the session for the same NAS-IP and Port. The next user logs in, but the system does not clean up the stale session nor does it replace the old data with the new data.</p> <p>Workaround: None</p>
CSCef53005	<p>Request with authorize only requested if no authentication service</p> <p>Symptom: A packet with a Service-Type of Authorize Only is rejected.</p> <p>Conditions: This might occur if no Authentication Service is specified.</p> <p>Workaround: Set a default Authentication Service (it will be ignored).</p>
CSCef81989	<p>Hot-configuration of session-cache resource manager broken</p> <p>Symptom: Implicit authentication requests fail or the server becomes unstable after making a modification to a server with a Trusted ID service.</p> <p>Conditions: A trace of the Trusted ID feature says that the query key cannot be found in the request packet, but the trace clearly shows that the key is there. Also, when the Trusted ID objects were added, no reload was given. The server will become unstable if any object is touched when there is a Trusted ID service configured. The server can core after a hot configuration of any server object.</p> <p>Workaround: Reload the server after adding the Trusted ID configuration or changing any configuration when a Trusted ID service is configured.</p>

Table 11 Anomalies Fixed in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeh19502	<p>Reverse zone name synthesis should use Framed-IP-Netmask</p> <p>Symptom: DDNS remove requests appear to be ignored by the DNS server after a session manager with multiple DDNS resource managers completes releasing resources.</p> <p>Conditions: The server is setup with multiple DDNS resource managers each containing the same forward zone, but a different reverse zone, to handle multiple, discrete IP pools in the network. When the accounting stop appears for a user, the forward zone still contains the mapping.</p> <p>Workaround: Split the DDNS resource managers such that you have one DDNS resource manager per session manager. Multiple sessions managers and a script to set the Session-Manager environment variable to use the correct pool are required.</p>
CSCeg27967	<p>Cannot set Response-Type to Accept in TCL script</p> <p>Symptom: A TCL script which sets the response type to Access-Accept ceases to work.</p> <p>Conditions: This might occur after an upgrade to Cisco AR 3.0R3 or later.</p> <p>Workaround: Define a Rex service which sets the response type to Access-Accept. This might be combined with another authentication service in a group service if necessary.</p>
CSCeg30580	<p>Unable to proxy session keys</p> <p>Symptom: Proxy is occasionally unable to reencrypt session keys.</p> <p>Conditions: AR is setup to proxy the MPPE attributes used as session keys in many EAP types.</p> <p>Workaround: None</p>
CSCeg43945	<p>Cisco AR authenticates the user although the username ends with slash character (/).</p> <p>Symptom: A username that ends with the slash character authenticates successfully.</p> <p>Conditions: A user attempts to authenticate with a username ending with a slash still authenticates successfully.</p> <p>Workaround: None</p>
CSCeg46256	<p>EAP-negotiate fails with EAP-SIM if EAP-SIM is not the first service</p> <p>Symptom: EAP-SIM authentication fails with EAP-Negotiate services.</p> <p>Conditions: The EAP-SIM service is not the first service in the configured service list of the EAP-Negotiate service.</p> <p>Workaround: Set the EAP-SIM service as the first service in the service list of the EAP-Negotiate service.</p>
CSCeg63826	<p>is835c_ebs_return_quota and is835c_ebs_reauthorize_quota not working</p> <p>Symptom: These two API library calls do not occur.</p> <p>Conditions: This will occur if you have IS 835C billing configured.</p> <p>Workaround: None.</p>
CSCeg73910	<p>DDNS update missed in Simple IP hand-off with Reverse zone server</p> <p>Symptom: DNS will not contain entry for the mobile node.</p> <p>Conditions: When the reverse zone is configured and Simple IP hand-off takes place.</p> <p>Workaround: None.</p>

Table 11 Anomalies Fixed in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeg88981	<p>Implicit login flag change does not have immediate effect</p> <p>Symptom: User passes an implicit login with Implicit-Auth-Enabled set to FALSE.</p> <p>Conditions: The Trusted ID flow is in use and the user's Implicit-Auth-Enabled has been changed from TRUE to FALSE. If the user is in the cache from a previous passing explicit login, the first implicit login request following the flag change will pass, but every one after will fail.</p> <p>Workaround: After changing the flag, manually remove the user from the cache using the <b>release-sessions</b> command in <b>aregcmd</b>.</p>
CSCeg90796	<p>AuthenticationTimeout property not validated for EAP-Negotiate</p> <p>Symptom: The AuthenticationTimeout property of EAP-Negotiate services is not validated.</p> <p>Conditions: An erroneous value is set for AuthenticationTimeout property of an EAP-Negotiate service.</p> <p>Workaround: Set only valid values (numeric value between 10 and 600) for the AuthenticationTimeout property.</p>
CSCeh04214	<p>TLS session not torn down for invalid IMSI for EAP-SIM with PEAP</p> <p>Symptom: The TLS session does not seem to be destroyed when an invalid IMSI is specified for PEAP authentication using the EAP-SIM inner method.</p> <p>Conditions: An invalid IMSI is specified in the authentication request.</p> <p>Workaround: Specify only valid IMSIs in authentication requests.</p>
CSCeh52128	<p>Invalid pointer values in <b>rexusr.cpp</b> after uninitialization</p> <p>Symptom: Server crashes on incoming requests after a configuration change that triggers a hot configuration.</p> <p>Conditions: <b>rexusr.cpp</b> is configured as the USRIncomingScript.</p> <p>Workaround: Modify the <b>rexusr.cpp</b> file with SE assistance.</p>
CSCeh56736	<p>Confusing log message 8692 of 8192 packets in use</p> <p>Symptom: A message similar to the following appears in the log file. Note that the number of used buffer is larger than the number of buffers configured in the buffer pool:</p> <pre>&lt;timestamp&gt; name/radius/1 Error Server 0 Radius has used 8692 of its 8192 request buffers: the server is dropping 1 request; 1 packets dropped total.</pre> <p>Conditions: The server is running under heavy load. On source code review, it was determined that this is merely a book-keeping error in the code that generates packet usage statistics and there is no problem with the actual packet handling or buffer management code.</p> <p>Workaround: None required. Ignore the message.</p>

Table 11 Anomalies Fixed in Cisco AR 4.0.1 (continued)

Bug	Description
CSCeh56788	<p>NULL packet pointer was passed to update stats function</p> <p>Symptom: Under some high load conditions, the server crashes. The core file points to a crash in RemoteRadiusServer::updateStats()</p> <p>Conditions: The server has run out of RADIUS packet buffers at the same time that a request to a remote server has timed out. The first condition normally generates a log message like this:</p> <pre>Error Server 0 Radius has used 8192 of its 8192 request buffers: the server is dropping 1 request; 1 packets dropped total.</pre> <p>Workaround: Reduce the load on the server or increase the size of the RADIUS packet buffer pool by setting <b>/Radius/Advanced/MaximumNumberOfRadiusPackets</b></p>
CSCin09020	<p>Incorrect Log message in agent_server_log when Cisco AR starts up</p> <p>Symptom: When Cisco AR server is restarted, the following message appears in the log:</p> <pre>could not get state serial number</pre> <p>This message does not indicate any problem and should not be a cause for concern.</p> <p>Conditions: This message occurs in the log when Cisco AR server is restarted.</p> <p>Workaround: None required.</p>

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section on page 6 section.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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. (0812R)

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.

© 2005-2008 Cisco Systems, Inc. All rights reserved.