

Using LDAP

Revised: March 20, 2009, OL-17222-03

This chapter provides information about using Lightweight Directory Access Protocol (LDAP) with Cisco Access Registrar (CAR) to access information directories. You can use CAR to authenticate and authorize access requests by querying user information through LDAP.



Note

CAR 4.2 supports LDAP version 3 and LDAP version 2 directory servers.

Configuring LDAP

To use LDAP in CAR, use **aregcmd** to do the following:

1. Configure an LDAP Service.
 - Configure an LDAP RemoteServer object.
 - Set LDAP service as the default AA service.
4. Save your configuration.

After you issue the **save** command, CAR attempts to validate the configuration, checks for all required properties, and ensures there is no logic error. If the validation is successful, CAR saves the configuration to the MCD database. When CAR is reloaded, it shuts down any current LDAP connections and builds new connections for the configured LDAP remote servers.

Configuring the LDAP Service

/Radius/Services

/Radius/Services

```
[ //localhost/Radius/Services/AR-LDAP ]
Name =
Description =
Type = ldap
IncomingScript~ =
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ =
MultipleServersPolicy = Failover
RemoteServers/
```

Table 19-1 describes the LDAP service properties.

Table 19-1 LDAP Service Properties

Parameter	Description
	Required; inherited from the upper directory
Description	An optional description of the service
Type	Must be set to LDAP for LDAP service
IncomingScript	Optional
OutgoingScript	Optional
OutagePolicy	Required; must be set to AcceptAll or Drop Packet, or defaults to RejectAll
OutageScript	Optional
MultipleServersPolicy	Required; must be set to RoundRobin or defaults to Failover.
RemoteServers	Required; list of one or more remote servers defined under <code>/Radius/RemoteServers</code> . These servers must be listed in order under

MultipleServersPolicy

Use the MultipleServersPolicy property to configure the LDAP remote servers in RoundRobin mode, or the default Failover mode applies. When set to Failover, CAR directs requests to the first server in the `/Radius/Services/LDAP/RemoteServers` requests to the next server in the list. The process continues until CAR locates an on-line server.

When set to RoundRobin, CAR directs each request to the next server in the RemoteServers list to share the resource load across all listed servers.

RemoteServers

`/Radius/RemoteServers`.

Configuring an LDAP RemoteServer

- Name
- Protocol
- Port
- HostName

BindName
 BindPassword
 SearchPath
 Filter

The following properties must be configured to enable Bind-Based Authentication:

Name
 Protocol
 Port
 HostName
 SearchPath
 Filter



You can leave the BindName, BindPassword, UserPasswordAttribute, PasswordEncryptionStyle and DNSLookupAndLDAPRebindInterval properties blank when you configure the Bind-Based Authentication feature in CAR.

Table 19-2 describes the LDAP Remote Server properties.

Table 19-2 LDAP Remote Server Properties

	Required; port on which LDAP server listens, default is port 389. If port is not set or set to zero, LDAP remote server will automatically be set to port 389.
ReactivateTimerInterval	Required; default is 300000 (ms)
Timeout	Required; specifies length of time CAR waits for a response from the LDAP server before noting the server as down; default is 15 (seconds)
HostName	Required; specifies the hostname, FQDN, or IP address of the LDAP server
BindName	Specifies the distinguished name (DN) in the LDAP server for CAR to bind with the LDAP server
BindPassword	Specifies the password for the distinguished name
UseSSL	FALSE by default
SearchPath~	Specifies search base to the organization and domain; for example: o=cisco.com
Filter~	(uid=%s) by default
UserPasswordAttribute	Should be set to the attribute in the directory server which stores users' passwords; default is <i>userpassword</i>

LDAPToEnvironmentMappings	<p>Optional; a list of name/value pairs in which the name is the name of the ldap attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the ldap attribute retrieved.</p> <p>For example, when the LDAPToEnvironmentMappings</p> <pre> group = User-Group ldap group User-Group </pre>
	<p style="text-align: center;"><i>attribute/value</i></p>

DNS Look Up and LDAP Rebind Interval

set DNSLookupAndLDAPRebindInterval 15M—



set DNSLookupAndLDAPRebindInterval 1h—performs DNS resolution every hour

Step 1

Step 2

set DNSLookupAndLDAPRebindInterval 30 M

LDAP Rebind Failures

LDAPToRadiusMappings

Values stored in a multi-valued field in the LDAP directory are mapped to multiple RADIUS attributes. For example, if the LDAPToRadiusMappings has the following entry:

```
tunnel-info = Cisco-AVPair
```

The following LDAP fields in the user's record will create four Cisco-AVPair attributes in the user's Access-Accept RADIUS packet:

```
tunnel-info: vpdn:tunnel-id=ssg001
tunnel-info: vpdn:tunnel-type=12tp
tunnel-info: vpdn:ip-addresses=10.2.2.2
tunnel-info: vpdn:12tp-tunnel-password=secret
```

LDAPToEnvironmentMappings

For example, when the LDAPToEnvironmentMappings has the entry: group =User-Group, the RemoteServer retrieves the attribute from the LDAP user entry for the specified user, uses the value returned, and sets the Environment variable User-Group to that value.

LDAPToCheckItemMappings

Setting LDAP As Authentication and Authorization Service

```
set DefaultAuthenticationService AR-LDAP
set DefaultAuthorizationService AR-LDAP
```

Saving Your Configuration

-
-
-

CHAP Interoperability with LDAP

Allowing Special Characters in LDAP Usernames

```
* ( ) \
```

```
aregcmd
/Radius/RemoteServers/ldap-server

cd /Radius/RemoteServers/ldap-server
set EscapeSpecialCharInUserName TRUE

/Radius/RemoteServers/Ldap-Server
EscapeSpecialCharInUserName = TRUE
```



Note

Dynamic LDAP Search Base

`rex.h`

`/Radius/IncomingScript`

```
set user [ $request get User-Name ]
if { [ regexp {^[^@]+@([^\.]+)\.(.+)$} $user m org domain ] } {
$environ put Dynamic-Search-Path "ou=$org,ou=people,o=$domain"
```

Analyzing LDAP Trace Logs

Successful Bind Message

`name_radius_1_trace`

```
10/23/2008 11:02:57: Log: Successfully bind to LDAP Server ldapserver (spatula-u5:389)
```

Bind Failure Messages

```
10/23/2008 11:10:50: Log: Write in LDAPClient returned an error (32)
```

```
10/23/2008 11:10:50: Log: Remote LDAP Server ldapserver (spatula-u5:387): Unable to
bind to LDAP Server: Can't contact LDAP server
```

```
10/23/2008 11:10:50: Log: Remote LDAP Server ldapserver (spatula-u5:387): Failed to
open the connection to the LDAP server
```

```
10/23/2008 11:45:14: Log: Remote LDAP Server ldapserver (spatula-u5:389): Unable to
bind to LDAP Server: No such object ()
```

10/23/2008 11:45:14: Log: Remote LDAP Server ldapserver (spatula-u5:389): Failed to open the connection to the LDAP server

10/23/2008 11:51:55: Log: Remote LDAP Server ldapserver (spatula-u5:389): Unable to bind to LDAP Server: Invalid credentials
10/23/2008 11:51:55: Log: Remote LDAP Server ldapserver (spatula-u5:389): Failed to open the connection to the LDAP server

jane

jane

10/23/2008 11:24:17: P8457: Authenticating and Authorizing with Service AR-LDAP
10/23/2008 11:24:17: id = 5
10/23/2008 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): Querying LDAP server, id = 5.
10/23/2008 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): GotLDAP response, id = 5.
10/23/2008 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): No matching entries returned from LDAP query.
10/23/2008 11:24:17: P8457: User jane was not found in the LDAP store
10/23/2008 11:24:17: P8457: Rejecting request
10/23/2008 11:24:17: P8457: Rejecting request
10/23/2008 11:24:17: P8457: Trace of Access-Reject packet
10/23/2008 11:24:17: P8457: identifier = 4
10/23/2008 11:24:17: P8457: length = 35
10/23/2008 11:24:17: P8457: reqauth = 01:ad:cf:c7:4f:8e:a4:38:b0:d8:0a:e5:3d:9f:64:16
10/23/2008 11:24:17: P8457: Reply-Message = Access Denied

bob

bob



Bind-Based Authentication for LDAP

Configuring Bind-Based Authentication for LDAP

Step 1

Step 2

```
[ //localhost/Radius ]
```

```
cd Services/
```

```
add ldap
```

```
cd ldap
```

```
set Type ldap
```

[//localhost/Radius/Services/ldap]

```
cd RemoteServers
add 1 ldapservers
```

[//localhost/Radius]

```
cd RemoteServers
add ldapservers
cd ldapservers
```

[//localhost/Radius/RemoteServers/ldap]

```
set Port <remote ldap server prt numer>
set HostName
set SearchPath configured in ldap server
set UseBindBasedAuthentication TRUE
cd /Radius
set DefaultAuthenticationService ldap service name
set DefaultAuthorizationService ldap service name
```

```
save
```

Step 5
