

LDAP Configuration Mode Commands

LDAP configuration mode commands allow you to configure multiple Lightweight Directory Access Protocol (v3) (LDAP) servers as a named AAA server group. You specify the IP address of one or more previously configured LDAP servers that you want added to or removed from a AAA server group with configuration parameters such as the user profile attribute, the base DN, and the filter to use in the search request.

For details about creating an LDAP server group, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

To create an LDAP server group and access the LDAP server configuration mode, use the **aaa group server ldap** command in configuration mode. The CLI prompt changes to (config-ldap). Use the **no** form of this command to remove an LDAP server group.

```
aaa group server ldap group_name
```

```
no aaa group server ldap group_name
```

Syntax Description

ldap	Specifies an LDAP directory server group.
<i>group_name</i>	Name for the group of LDAP servers. The server group name is a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A server group is a list of server hosts. The ACE allows you to configure multiple AAA servers as a named server group. You group the different AAA server hosts into distinct lists. The ACE searches for the server hosts in the order in which you specify them within a group. You can configure a maximum of 100 server groups for each context in the ACE.

You can configure LDAP server groups at any time, but you must enter the **aaa authentication login** command to apply the groups to the AAA service.

Examples

To create an LDAP server group, enter:

```
host1/Admin(config) aaa group server ldap LDAP_Server_Group1  
host1/Admin(config-ldap) # server 172.16.56.76  
host1/Admin(config-ldap) # server 172.16.56.77  
host1/Admin(config-ldap) # server 172.16.56.78
```

Related Commands

[\(config\) aaa authentication login](#)

(config-ldap) attribute user-profile

To specify the user profile attribute that the Lightweight Directory Access Protocol (LDAP) server group uses, use the **attribute user-profile** command. Use the **no** form of this command to delete a user profile attribute from the LDAP server group.

attribute user-profile *text*

no attribute user-profile *text*

Syntax Description

<i>text</i>	User profile. The user profile is an unquoted text string of a maximum of 63 alphanumeric characters without spaces.
-------------	--

Command Modes

LDAP configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The user profile attribute type is a mandatory configuration for an LDAP server group. Without this setting, the user profile attribute cannot be retrieved by the LDAP server.

The user profile attribute type is a private attribute. In this case, the LDAP server database should use the same attribute type for the user profile. The LDAP client (the ACE) sends the search request with this attribute type as the attribute that it wants to download. If the lookup was successful, the search response contains this attribute value. The attribute value should contain a string that represents the user role and domain pair for this particular context.

Examples

To configure a user profile attribute for the LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# attribute user-profile usrprof
```

Related Commands

[\(config\) aaa group server](#)

(config-ldap) baseDN

To configure the base distinguished name (DN) that you want to use to perform search operations in the LDAP directory tree, use the **baseDN** command. A baseDN can take a form such as `dc=your,dc=domain`, where the base DN uses the DNS domain name as its basis and is split into the domain components. Use the **no** form of this command to delete a configured baseDN for the LDAP server group.

baseDN *text*

no baseDN *text*

Syntax Description	<i>text</i> Distinguished name of the search base. The baseDN name is a quoted text string of a maximum of 63 alphanumeric characters without spaces.
---------------------------	---

Command Modes	LDAP configuration mode Admin and user contexts
----------------------	--

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	The base DN is a mandatory configuration for an LDAP server group. Without this setting, a user cannot be authenticated.
-------------------------	--

Examples	<p>To configure the base DN for the LDAP server group, enter:</p> <pre>host1/Admin(config)# aaa group server ldap LDAP_Server_Group1 host1/Admin(config-ldap)# baseDN "dc=sns,dc=cisco,dc=com"</pre> <p>To delete the configured base DN, enter:</p> <pre>host1/Admin(config-ldap)# no baseDN "dc=sns,dc=cisco,dc=com"</pre>
-----------------	---

Related Commands	(config) aaa group server
-------------------------	---

(config-ldap) filter search-user

To configure a search request sent by the Lightweight Directory Access Protocol (LDAP) client to the server to find the user's node in the Directory Information Tree (DIT), use the **filter search-user** command. The \$user and \$contextid are substituted with actual values when sending the request. Use the **no** form of the command to delete the search request from the LDAP server group.

filter search-user *text*

no filter search-user *text*

Syntax Description	<i>text</i> Search request. The search filter is a quoted text string of a maximum of 63 alphanumeric characters without spaces.
---------------------------	--

Command Modes	LDAP configuration mode Admin and user contexts
----------------------	--

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	<p>The search filter is a mandatory configuration for an LDAP server group. Without this setting, a user cannot be authenticated.</p> <p>The search filter should follow the format defined in RFC 2254. The LDAP client sends the search request with the configured search filter after replacing the \$userid and \$contextid with the userid that the client is trying to authenticate and the associated virtual context name. The ACE allows \$userid and \$contextid to be used as placeholders for user ID and context ID.</p>
-------------------------	--

Examples	<p>To configure a search request for the LDAP server group, enter:</p> <pre>host1/Admin(config)# aaa group server ldap LDAP_Server_Group1 host1/Admin(config-ldap)# filter search-user "(&(objectclass=person) (&(cn=\$userid)(cid=\$contextid)))"</pre>
-----------------	--

To delete the search request, enter:

```
host1/Admin(config-ldap)# no filter search-user
"(&(objectclass=person)(&(cn=$userid)(cid=$contextid)))"
```

Related Commands	(config) aaa group server
-------------------------	---

(config-ldap) server

To specify the IP address of one or more previously configured Lightweight Directory Access Protocol (LDAP) servers that you want added to or removed from the AAA server group, use the **server** command. Use the **no** form of this command to remove the server from the AAA server group.

server *ip_address*

no server *ip_address*

Syntax Description

ip_address IP address of the LDAP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

LDAP configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can add multiple LDAP servers to the AAA server group by entering multiple **server** commands while in this mode. The same server can belong to multiple server groups.

Examples

To add one or more servers to an LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# server 172.16.56.76
host1/Admin(config-ldap)# server 172.16.56.79
host1/Admin(config-ldap)# server 172.16.56.82
```

To remove a server from the LDAP server group, enter:

```
host1/Admin(config-ldap)# no server 172.16.56.76
```

Related Commands

[\(config\) aaa group server](#)