CHAPTER 18

ldap-attribute-map through log-adj-changes Commands

ldap-attribute-map (aaa-server host mode)

To bind an existing mapping configuration to an LDAP host, use the **ldap-attribute-map** command in aaa-server host mode.

To remove the binding, use the **no** form of this command.

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

Syntax Description

map-name	Specifies an LDAP attribute mapping configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

If the Cisco-defined LDAP attribute names do not meet your ease-of-use or other requirements, you can create your own attribute names, map them to Cisco attributes, and then bind the resulting attribute configuration to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This command enters ldap-attribute-map mode. Note that there is no hyphen after “ldap” in this command.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute mapping configuration.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map configuration to an LDAP server.

Examples

The following example commands, entered in aaa-server host configuration mode, bind an existing attribute map named myldapmap to an LDAP server named ldapsvr1:

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running ldap attribute mapping configuration or all running attribute mapping configurations.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

ldap attribute-map (global configuration mode)

To create and name an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names, use the **ldap attribute-map** command in global configuration mode.

To remove the map, use the **no** form of this command.

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

Syntax Description

map-name	Specifies a user-defined name for an LDAP attribute map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **ldap attribute-map** command, you can map your own attribute names and values to Cisco attribute names. You can then bind the resulting attribute map to an LDAP server. Your typical steps would be as follows:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after ldap in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example command, entered in global configuration mode, creates an LDAP attribute map named myldapmap prior to populating it or binding it to an LDAP server:

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name to a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to the Cisco attribute name.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

ldap-base-dn

To specify the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request, use the **ldap-base-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, thus resetting the search to start at the top of the list, use the **no** form of this command.

ldap-base-dn *string*

no ldap-base-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request; for example, OU=Cisco. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

Start the search at the top of the list.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Pre-existing command, modified for this release

Usage Guidelines

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP base DN as starthere.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN.

ldap-defaults

To define LDAP default values, use the **ldap-defaults** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These default values are used only when the LDAP server requires them. To specify no LDAP defaults, use the **no** form of this command.

ldap-defaults *server* [*port*]

no ldap-defaults

Syntax Description

port	(Optional) Specifies the LDAP server port. If this parameter is not specified, the security appliance uses the standard LDAP port (389).
server	Specifies the IP address or domain name of the LDAP server. If one exists within the CRL distribution point, it overrides this value.

Defaults

The default setting is not set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example defines LDAP default values on the default port (389):

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs

ldap-dn

To pass a X.500 distinguished name and password to an LDAP server that requires authentication for CRL retrieval, use the **ldap-dn** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

To specify no LDAP DN, use the **no** form of this command.

ldap-dn *x.500-name password*

no ldap-dn

Syntax Description

password	Defines a password for this distinguished name. The maximum field length is 128 characters.
x.500-name	Defines the directory path to access this CRL database, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum field length is 128 characters.

Defaults

The default setting is not on.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example specifies an X.500 name CN=admin,OU=devtest,O=engineering and a password xxzzyy for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

Related Commands

Command	Description
crl configure	Enters crl configure configuration mode.

Command	Description
crypto ca trustpoint	Enters ca trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

ldap-login-dn

To specify the name of the directory object that the system should bind this as, use the **ldap-login-dn** command in aaa-server host mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-login-dn *string*

no ldap-login-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0 (1)	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Some LDAP servers, including the Microsoft Active Directory server, require that the security applianceestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the security appliance. These characteristics should correspond to those of a user with administrator privileges.

For the *string* variable, enter the name of the directory object for VPN Concentrator authenticated binding, for example: cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com. For anonymous access, leave this field blank.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login DN as myobjectname.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-login-password

To specify the login password for the LDAP server, use the **ldap-login-password** command in aaa-server host mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this password specification, use the **no** form of this command:

ldap-login-password *string*

no ldap-login-password

Syntax Description

string	A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum password string length is 64 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login password as obscurepassword.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-naming-attribute

To specify the Relative Distinguished Name attribute, use the **ldap-naming-attribute** command in aaa-server host mode. Aaa-server host configuration mode is accessible from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-naming-attribute *string*

no ldap-naming-attribute

Syntax Description

string	The case-sensitive, alphanumeric Relative Distinguished Name attribute consisting of up to 128 characters, that uniquely identifies an entry on the LDAP server. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP naming attribute as cn.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-over-ssl

To establish a secure SSL connection between the security appliance and the LDAP server, use the **ldap-over-ssl** command in aaa-server host configuration mode.

To disable SSL for the connection, use the **no** form of this command.

ldap-over-ssl enable

no ldap-over-ssl enable

Syntax Description

enable	Specifies that SSL secures a connection to an LDAP server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to specify that SSL secures a connection between the security appliance and an LDAP server.

Note We recommend enabling this feature if you are using plain text authentication. See the **sasl-mechanism** command.

Examples

The following commands, entered in aaa-server host configuration mode, enable SSL for a connection between the security appliance and the LDAP server named ldapsvr1 at IP address 10.10.0.1. They also configure the plain SASL authentication mechanism.

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
sasl-mechanism	Specifies SASL authentication between the LDAP client and server.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

ldap-scope

To specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request, use the **ldap-scope** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-scope *scope*

no ldap-scope

Syntax Description

scope	The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values are: • **onelevel**—Search only one level beneath the Base DN • **subtree**—Search all levels beneath the Base DN

Defaults

The default value is **onelevel**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Pre-existing command, modified for this release

Usage Guidelines

Specifying the scope as **onelevel** results in a faster search, because only one level beneath the Base DN is searched. Specifying **subtree** is slower, because all levels beneath the Base DN are searched.

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP scope to include the subtree levels.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.

leap-bypass

To enable LEAP Bypass, use the **leap-bypass enable** command in group-policy configuration mode. To disable LEAP Bypass, use the **leap-bypass disable** command. To remove the LEAP Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for LEAP Bypass from another group policy.

LEAP Bypass lets LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.

leap-bypass {**enable** | **disable**}

no leap-bypass

Syntax Description

disable	Disables LEAP Bypass.
enable	Enables LEAP Bypass.

Defaults

LEAP Bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This feature does not work as intended if you enable interactive hardware client authentication.

For further information, see the *Cisco Security Appliance Command Line Configuration Guide*.

Note There may be security risks in allowing any unauthenticated traffic to traverse the tunnel.

Examples

The following example shows how to set LEAP Bypass for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

Related Commands

Command	Description
secure-unit-authentication	Requires VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel.
user-authentication	Requires users behind VPN hardware clients to identify themselves to the security appliance before connecting.

lmfactor

To set a revalidation policy for caching objects that have only the last-modified timestamp, and no other server-set expiration values, use the **lmfactor** command in cache mode. To set a new policy for revalidating such objects, use the command again. To reset the attribute to the default value of 20, enter the **no** version of the command.

lmfactor *value*

no lmfactor

Syntax Description

value	An integer in the range of 0 to 100.

Defaults

The default value is 20.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Cache mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The security appliance uses the value of the lmfactor to estimate the length of time for which it considers a cached object to be unchanged. This is known as the expiration time. The security appliance estimates th expiration time by the time elapsed since the last modification multiplied by the lmfactor.

Setting the lmfactor to zero is equivalent to forcing an immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

Examples

The following example shows how to set an lmfactor of 30:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

log-adj-changes

To configure the router to send a syslog message when an OSPF neighbor goes up or down, use the **log-adj-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **log-adj-changes** command is enabled by default; it appears in the running configuration unless removed with the **no** form of the command.

Examples

The following example disables the sending of a syslog message when an OSPF neighbor goes up or down:

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.