CHAPTER 18

ldap-base-dn through log-adj-changes Commands

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
3.1(1)	This command was introduced.

Usage Guidelines

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 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 that 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 FWSM 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
3.1(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
3.1(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
3.1(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 FWSM establish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The FWSM 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 FWSM. 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 a RADIUS 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))# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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
3.1(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 a RADIUS 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 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)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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 (or attributes), use the **ldap-naming-attribute** 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-naming-attribute *string*

no ldap-naming-attribute

Syntax Description

string	The case-sensitive, alphanumeric Relative Distinguished Name attribute (or attributes), 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
3.1(1)	This command was introduced.

Usage Guidelines

Enter the Relative Distinguished Name attribute (or attributes) 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 a RADIUS 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 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)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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-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 configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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 a RADIUS AAA server named “svrgrp1” on host “209.165. 200.225”, 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 209.165.200.225
hostname(config-aaa-server-host# timeout 9
hostname(config-aaa-server-host)# retry 7
```

```
hostname(config-aaa-serve-host)# ldap-scope subtree
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters aaa server host configuration mode so that 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 {**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
3.1(1)	This command was introduced.

Usage Guidelines

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.

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

For further information, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module 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 FWSM before connecting.

limit-resource

To specify a resource limit for a class in multiple context mode, use the **limit-resource** command in class configuration mode. To restore the limit to the default, use the **no** form of this command. The FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

limit-resource {**all** {*number***%** | **0**} | [**rate**] *resource_name number*[**%**] | **0**}

no limit-resource {**all** | [**rate**] *resource_name*}

Syntax Description

0	Sets the resource to unlimited (the system limit).
all	Sets the limit for all resources, as a percentage, or as unlimited.
number[**%**]	Specifies the resource limit as a fixed number greater than or equal to 1, or as a percentage of the system limit (when used with the percent sign (%)). You can assign more than 100 percent if you want to oversubscribe the device. For **all** resources, you can only set a percentage or **0** for unlimited.
rate	Specifies that you want to set the rate per second for a resource for which you can set either the rate or an absolute limit. See Table 18-1 for resources for which you can set the rate per second.
resource_name	Specifies the resource name for which you want to set a limit. This limit overrides the limit set for **all**.

Defaults

All resources are set to unlimited, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- IPSec sessions—5 sessions.
- MAC addresses—65,535 entries.

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**
Class configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

When you limit a resource for a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can "use up" those resources, potentially affecting service to other contexts.

Table 18-1 lists the resource types and the limits. See also the **show resource types** command.

Table 18-1 Resource Names and Limits

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
mac-addresses	N/A	65 K concurrent	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	N/A	999,900 concurrent 170,000 per second (rate)	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. **Note** For concurrent connections, the FWSM allocates half of the limit to each of two network processors (NPs) that accept connections. Typically, the connections are divided evenly between the NPs. However, in some circumstances, the connections are not evenly divided, and you might reach the maximum connection limit on one NP before reaching the maximum on the other. In this case, the maximum connections allowed is less than the limit you set. The NP distribution is controlled by the switch based on an algorithm. You can adjust this algorithm on the switch, or you can adjust the connection limit upward to account for the inequity.
fixups	N/A	100,000 per second (rate)	Application inspection.
hosts	N/A	256 K concurrent	Hosts that can connect through the FWSM.
ipsec	1 minimum 5 maximum concurrent	10 concurrent	IPSec sessions
asdm	1 minimum 5 maximum concurrent	32 concurrent	ASDM management sessions. **Note** ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions.
ssh	1 minimum 5 maximum concurrent	100 concurrent	SSH sessions.

Table 18-1 Resource Names and Limits (continued)

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
syslogs	N/A	30,000 per second (rate)	System messages. **Note** The FWSM can support 30,000 messages per second for messages sent to the FWSM terminal or buffer. If you send messages to a syslog server, the FWSM supports 25,000 per second.
telnet	1 minimum 5 maximum concurrent	100 concurrent	Telnet sessions.
xlates	N/A	256 K concurrent	NAT translations.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold with all resources set to 5 percent, except for fixups, with a setting of 10 percent, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

To add a class called silver with all resources set to 3 percent, except for system log messages, with a setting of 500 per second, enter the following commands:

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
member	Assigns a context to a resource class.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

log

When using the Modular Policy Framework, log packets that match a **match** command or class map by using the **log** command in match or class configuration mode. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. This log action is available in an inspection policy map for application traffic. To disable this action, use the **no** form of this command.

log

no log

Syntax Description

This command has no arguments or keywords.

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
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **log** command to log all packets that match the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http** *http_policy_map* command where *http_policy_map* is the name of the inspection policy map.

Examples

The following example sends a log when packets match the http-traffic class map.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

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
1.1(1)	This command was introduced.

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.