CHAPTER 17

l2tp tunnel hello through log-adj-changes Commands

l2tp tunnel hello

To specify the interval between hello messages on L2TP over IPSec connections, use the **l2tp tunnel hello** command in global configuration mode. To reset the interval to the default, use the **no** form of the command:

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

Syntax Description

interval	Interval between hello messages in seconds. The Default is 60 seconds. The range is 10 to 300 seconds.

Defaults

The default is 60 seconds.

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
7.2(1)	This command was introduced.

Usage Guidelines

The **l2tp tunnel hello** command enables the adaptive security appliance to detect problems with the physical layer of the L2TP connection. The default is 60 secs. If you configure it to a lower value, connections that are experiencing problems are disconnected earlier.

Examples

The following example configures the interval between hello messages to 30 seconds:

```
hostname(config)# l2tp tunnel hello 30
```

Related Commands

Command	Description
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	Displays the details of L2TP connections.
vpn-tunnel-protocol l2tp-ipsec	Enables L2TP as a tunneling protocol for a specific tunnel group.

ldap attribute-map

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-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 configuration 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-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 configuration	•	•	•	•	—

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

ldap-group-base-dn

To specify the base group in the Active Directory hierarchy used by dynamic access policies for group searches, use the **ldap-group-base-dn** command in aaa-server host configuration mode. To remove the command from the running configuration, use the **no** form of the command:

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the location in the Active Directory hierarchy where the server should begin searching. For example, ou=Employees. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behavior or values. If you do not specify a group search DN, the search begins at the base DN.

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 mode	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **ldap-group-base-dn** command applies only to Active Directory servers using LDAP, and specifies an Active Directory heirarchy level that the **show ad-groups** command uses to begin its group search. The groups retrieved from the search are used by dynamic group policies as selection criteria for a specific policy.

Examples

The following example sets the group base DN to begin the search at the organization unit (ou) level Employees:

```
hostname(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

Related Commands

Command	Description
group-search-timeout	Adjusts the time the adaptive security appliance waits for a response from an Active Directory server for a list of groups.
show ad-groups	Displays groups that are listed on an Active Directory server.

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 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-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 configuration	•	•	•	•	—

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 adaptive security applianceestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The adaptive 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 adaptive 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 configuration 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 configuration	•	•	•	•	—

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 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-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 configuration	•	•	•	•	—

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 adaptive 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 adaptive 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 adaptive 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 configuration	•	•	•	•	—

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 {**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

When enabled, LEAP Bypass allows LEAP packets from wireless devices behind a VPN hardware client to travel across a VPN tunnel prior to user authentication. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Devices are then able to authenticate again, per user authentication.

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

For further information, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

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 adaptive security appliance before connecting.

license-server address

To identify the shared licensing server IP address and shared secret for use by a participant, use the **license-server address** command in global configuration mode. To disable participation in shared licensing, use the **no** form of this command. A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed amongst a group of adaptive security appliances by configuring one of the adaptive security appliances as a shared licensing server, and the rest as shared licensing participants.

license-server address *address* **secret** *secret* [**port** *port*]

no license-server address [*address* **secret** *secret* [**port** *port*]]

Syntax Description

address	Identifies the shared licensing server IP address.
port *port*	(Optional) If you changed the default port in the server configuration using the **license-server port** command, set the port for the backup server to match, between 1 and 65535. The default port is 50554.
secret *secret*	Identifies the shared secret. The secret muct match the secret set on the server using the **license-server secret** command.

Command Default

The default port is 50554.

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
8.2(1)	This command was introduced.

Usage Guidelines

The shared licensing participant must have a shared licensing participant key. Use the **show activation-key** command to check your installed licenses.

You can only specify one shared license server for each participant.

The following steps describe how shared licenses operate:

1. Decide which adaptive security appliance should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which adaptive security appliances should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.

3. (Optional) Designate a second adaptive security appliance as a shared licensing backup server. You can only specify one backup server.

   Note The shared licensing backup server only needs a participant license.

4. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
5. When you configure the adaptive security appliance as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

   Note The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

6. The shared licensing server responds with information about how often the participant should poll the server.
7. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
8. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

   Note The shared licensing server can also participate in the shared license pool if it runs out of local sessions. It does not need a participant license as well as the server license to participate.

   a. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
   b. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
9. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The adaptive security appliance uses SSL between the server and participant to encrypt all communications.

Communication Issues Between Participant and Server

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.
- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.

- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

Examples

The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
hostname(config)# license-server address 10.1.1.1 secret farscape
hostname(config)# license-server backup address 10.1.1.2
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup address

To identify the shared licensing backup server IP address for use by a participant, use the **license-server backup address** command in global configuration mode. To disable use of the backup server, use the **no** form of this command.

license-server backup address *address*

no license-server address [*address*]

Syntax Description

address	Identifies the shared licensing backup server IP address.

Command Default

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
8.2(1)	This command was introduced.

Usage Guidelines

The shared licensing backup server must have the **license-server backup enable** command configured.

Examples

The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
hostname(config)# license-server address 10.1.1.1 secret farscape
hostname(config)# license-server backup address 10.1.1.2
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.

Command	Description
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup backup-id

To identify the shared licensing backup server in the main shared licensing server configuration, use the **license-server backup backup-id** command in global configuration mode. To remove the backup server configuration, use the **no** form of this command.

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

Syntax Description

address	Identifies the shared licensing backup server IP address.
backup-id *serial_number*	Identifies the shared licensing backup server serial number.
ha-backup-id *ha_serial_number*	If you use failover for the backup server, identifies the secondary shared licensing backup server serial number.

Command Default

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
8.2(1)	This command was introduced.

Usage Guidelines

You can only identify 1 backup server and its optional standby unit.

To view the backup server serial number, enter the **show activation-key** command.

To enable a participant to be the backup server, use the **license-server backup enable** command.

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

Note When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server "recharges" up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server backup enable

To enable this unit to be the shared licensing backup server, use the **license-server backup enable** command in global configuration mode. To disable the backup server, use the **no** form of this command.

license-server backup enable *interface_name*

no license-server enable *interface_name*

Syntax Description

interface_name	Specifies the interface on which participants contact the backup server. You can repeat this command for as many interfaces as desired.

Command Default

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
8.2(1)	This command was introduced.

Usage Guidelines

The backup server must have a shared licensing participant key.

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

Note When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server "recharges" up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.

Examples

The following example identifies the license server and shared secret, and enables this unit as the backup shared license server on the inside interface and dmz interface.

```
hostname(config)# license-server address 10.1.1.1 secret farscape
hostname(config)# license-server backup enable inside
hostname(config)# license-server backup enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server enable

To identify this unit as a shared licensing server, use the **license-server enable** command in global configuration mode. To disable the shared licensing server, use the **no** form of this command. A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed amongst a group of adaptive security appliances by configuring one of the adaptive security appliances as a shared licensing server, and the rest as shared licensing participants.

license-server enable *interface_name*

no license-server enable *interface_name*

Syntax Description

interface_name	Specifies the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

Command Default

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
8.2(1)	This command was introduced.

Usage Guidelines

The shared licensing server must have a shared licensing server key. Use the **show activation-key** command to check your installed licenses.

The following steps describe how shared licenses operate:

1. Decide which adaptive security appliance should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which adaptive security appliances should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.
3. (Optional) Designate a second adaptive security appliance as a shared licensing backup server. You can only specify one backup server.

Note The shared licensing backup server only needs a participant license.

4. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
5. When you configure the adaptive security appliance as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

   Note The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

6. The shared licensing server responds with information about how often the participant should poll the server.
7. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
8. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

   Note The shared licensing server can also participate in the shared license pool if it runs out of local sessions. It does not need a participant license as well as the server license to participate.

   a. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
   b. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
9. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The adaptive security appliance uses SSL between the server and participant to encrypt all communications.

Communication Issues Between Participant and Server

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.
- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.
- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server port

To set the port on which the shared licensing server listens for SSL connections from participants, use the **license-server port** command in global configuration mode. To restore the default port, use the **no** form of this command.

license-server port *port*

no license-server port [*port*]

Syntax Description

seconds	Sets the port on which the server listens for SSL connections from participants, between 1 and 65535. The default is TCP port 50554.

Command Default

The default port is 50554.

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
8.2(1)	This command was introduced.

Usage Guidelines

If you change the port from the default, be sure to set the same port for each participant using the **license-server address** command.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server refresh-interval

To set the refresh interval provided to participants to set how often they should communicate with the shared licensing server, use the **license-server refresh-interval** command in global configuration mode. To restore the default refresh interval, use the **no** form of this command.

license-server refresh-interval *seconds*

no license-server refresh-interval [*seconds*]

Syntax Description

seconds	Sets the refresh interval between 10 and 300 seconds. The default is 30 seconds.

Command Default

The default is 30 seconds.

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
8.2(1)	This command was introduced.

Usage Guidelines

Each participant regularly communicates with the shared licensing server using SSL so the shared licensing server can keep track of current license usage and receive and respond to license requests.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

license-server secret

To set the shared secret on the shared licensing server, use the **license-server secret** command in global configuration mode. To remove the secret, use the **no** form of this command.

license-server secret *secret*

no license-server secret *secret*

Syntax Description

secret	Sets the shared secret, a string between 4 and 128 ASCII characters.

Command Default

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
8.2(1)	This command was introduced.

Usage Guidelines

Any participant with this secret identified in the **license-server address** command can use the licensing server.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface:

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.

Command	Description
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show shared license	Shows shared license statistics.
show vpn-sessiondb	Shows license information about VPN sessions.

lifetime (ca server mode)

To specify the length of time that the Local Certificate Authority (CA) certificate, each issued user certificates, or the Certificate Revocation List (CRL) is valid, use the **lifetime** command in CA server configuration mode. To reset the lifetime to the default setting, use the **no** form of this command.

lifetime {ca-certificate | certificate | crl} *time*

no lifetime {**ca-certificate | certificate | crl**}

Syntax Description

ca-certificate	Specifies the lifetime of the local CA server certificate.
certificate	Specifies the lifetime of all user certificates issued by the CA server.
crl	Specifies the lifetime of the CRL.
time	For the CA certificate and all issued certificates, *time* specifies the number of days the certificate is valid. The valid range is from 1 to 3650 days. For the CRL, *time* specifies the number of hours the CRL is valid. The valid range for the CRL is from 1 to 720 hours.

Defaults

The default lifetimes are:

- CA certificate - Three years
- Issued certificates - One year
- CRL - Six hours

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**
CA server configuration	•	—	•	—	—

Command History

Release	**Modification**
8.0(2)	This command was introduced.

Usage Guidelines

By specifying the number of days or hours that a certificate or CRL is valid, this command determines the expiration date included in the certificate or the CRL.

Examples

The following example configures the CA to issue certificates that are valid for three months:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime certificate 90
hostname(config-ca-server))#
```

The following example configures the CA to issue a CRL that is valid for two days:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime crl 48
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point (CDP) to be include in the certificates issued by the CA.
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
show crypto ca server	Displays the local CA configuration details in ASCII text.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server crl	Displays the current CRL of the local CA.

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 adaptive security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

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

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

Syntax Description

all 0	Sets the limit for all resources 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 between 1 and 100 (when used with the percent sign (%)). Set the limit to **0** to indicate an unlimited resource. For resources that do not have a system limit, you cannot set the percentage (%); you can only set an absolute value.
rate	Specifies that you want to set the rate per second for a resource. See Table 17-1 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	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you limit a resource for a class, the adaptive security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the adaptive security appliance 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 17-1 lists the resource types and the limits. See also the **show resource types** command.

Table 17-1 Resource Names and Limits

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
mac-addresses	Concurrent	N/A	65,535	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	Concurrent or Rate	N/A	Concurrent connections: See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for the connection limit for your platform. Rate: N/A	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
inspects	Rate	N/A	N/A	Application inspections.
hosts	Concurrent	N/A	N/A	Hosts that can connect through the adaptive security appliance.
asdm	Concurrent	1 minimum 5 maximum	32	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	Concurrent	1 minimum 5 maximum	100	SSH sessions.
syslogs	Rate	N/A	N/A	System log messages.
telnet	Concurrent	1 minimum 5 maximum	100	Telnet sessions.
xlates	Concurrent	N/A	N/A	Address translations.

[1] If this column value is N/A, then you cannot set a percentage of the resource because there is no hard system limit for the resource.

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, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

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.

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 configuration 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 configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The adaptive 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 adaptive 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

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. This log action is available in an inspection policy map (the **policy-map type inspect** command) 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
7.2(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
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.