

## **I2tp tunnel hello through log-adj-changes Commands**

---

# I2tp tunnel hello

To specify the interval between hello messages on L2TP over IPsec connections, use the **i2tp tunnel hello** command in global configuration mode. To remove the command from the configuration and set the default, use the no form of the command:

**i2tp tunnel hello** *interval*

**no i2tp 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:

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

## Command History

Release	Modification
7.2(1)	This command was introduced.

## Usage Guidelines

The **i2tp tunnel hello** command enables the 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)# i2tp tunnel hello 30
```

## Related Commands

Command	Description
<b>show vpn-sessiondbdetail remote filter protocol L2TPOverIPsec</b>	Displays the details of L2TP connections.
<b>vpn-tunnel-protocol i2tp-ipsec</b>	Enables L2TP as a tunneling protocol for a specific tunnel group.

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

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

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

**ldap-attribute-map** *map-name*

**no ldap-attribute-map** *map-name*

## Syntax Description

*map-name* Specifies an LDAP attribute mapping configuration.

## Defaults

No default behavior or values.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
	<b>ldap attribute-map (global configuration mode)</b>	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
	<b>map-name</b>	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
	<b>map-value</b>	Maps a user-defined attribute value to a Cisco attribute.
	<b>show running-config ldap attribute-map</b>	Displays a specific running ldap attribute mapping configuration or all running attribute mapping configurations.
	<b>clear configure ldap attribute-map</b>	Removes all LDAP attribute maps.

## ldap attribute-map (global configuration mode)

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

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

```
ldap attribute-map map-name
```

```
no ldap attribute-map map-name
```

### Syntax Description

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

### Defaults

No default behavior or values.

### Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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 command 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
<b>ldap-attribute-map (aaa-server host mode)</b>	Binds an LDAP attribute map to an LDAP server.
<b>map-name</b>	Maps a user-defined LDAP attribute name to a Cisco LDAP attribute name.
<b>map-value</b>	Maps a user-defined attribute value to the Cisco attribute name.
<b>show running-config ldap attribute-map</b>	Displays a specific running LDAP attribute map or all running attribute maps.
<b>clear configure ldap attribute-map</b>	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 accessible 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:

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

## Command History

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

## Usage Guidelines

This command is valid only for LDAP servers.

## Examples

The following example configures an LDAP AAA server named 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**

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

## ldap-defaults

To define LDAP default values, use the **ldap-defaults** command in `crl` configuration mode. `Crl` 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

<i>port</i>	(Optional) Specifies the LDAP server port. If this parameter is not specified, the security appliance uses the standard LDAP port (389).
<i>server</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>crl configure</b>	Enters <code>ca-crl</code> configuration mode.
<b>crypto ca trustpoint</b>	Enters trustpoint configuration mode.
<b>protocol ldap</b>	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

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>crl configure</b>	Enters <code>crl configure</code> configuration mode.

<b>Command</b>	<b>Description</b>
<b>crypto ca trustpoint</b>	Enters ca trustpoint configuration mode.
<b>protocol ldap</b>	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 accessible 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

<i>string</i>	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:

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

## Command History

Release	Modification
7.0	This command was introduced.
(1)	

## Usage Guidelines

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

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

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

## Examples

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

```

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

```

**Related Commands**

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

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

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

## Examples

The following example configures an LDAP AAA server named 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)#
```

## Related Commands

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

# ldap-naming-attribute

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

```
ldap-naming-attribute string
```

```
no ldap-naming-attribute
```

## Syntax Description

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

## Defaults

No default behaviors or values.

## Command Modes

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

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

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

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

## Examples

The following example configures an LDAP AAA server named 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)#
```

## Related Commands

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

# ldap-over-ssl

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

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

**ldap-over-ssl enable**

**no ldap-over-ssl enable**

## Syntax Description

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

## Defaults

No default behavior or values.

## Command Modes

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

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

## Command History

Release	Modification
7.1(1)	This command was introduced.

## Usage Guidelines

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



### Note

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

## Examples

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

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

## Related Commands

Command	Description
<b>sasl-mechanism</b>	Specifies SASL authentication between the LDAP client and server.
<b>server-type</b>	Specifies the LDAP server vendor as either Microsoft or Sun.
<b>ldap attribute-map (global configuration mode)</b>	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 accessible 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

<i>scope</i>	The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values are: <ul style="list-style-type: none"> <li>• <b>onelevel</b>—Search only one level beneath the Base DN</li> <li>• <b>subtree</b>—Search all levels beneath the Base DN</li> </ul>
--------------	--

## Defaults

The default value is **onelevel**.

## Command Modes

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

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

## Command History

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

## Usage Guidelines

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

This command is valid only for LDAP servers.

## Examples

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

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

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

# leap-bypass

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

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

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

**no leap-bypass**

## Syntax Description

<b>disable</b>	Disables LEAP Bypass.
<b>enable</b>	Enables LEAP Bypass.

## Defaults

LEAP Bypass is disabled.

## Command Modes

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

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

This feature does not work as intended if you enable interactive hardware client authentication. For further information, see the *Cisco Security Appliance Command Line Configuration Guide*.



### Note

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

## Examples

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

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

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

# lifetime

To specify the lifetime of an IKE security association before it expires, use the **lifetime** command in crypto isakmp policy configuration configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. Use the **no** form of this command to reset the security association lifetime to the default value of 86,400 seconds (one day).

**lifetime** *seconds*

**no lifetime**

## Syntax Description

<i>priority</i>	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
<i>seconds</i>	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for infinite lifetime.

## Defaults

The default value is 86,400 seconds (one day).

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto isakmp policy configuration	•	—	•	—	—

## Command History

Release	Modification
7.0(1)(1)	The <b>isakmp policy lifetime</b> command was preexisting.
7.2.(1)	The <b>lifetime</b> command replaces the <b>isakmp policy lifetime</b> command.

## Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPsec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the security appliance sets up future IPsec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

**Note**

If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

**Examples**

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 0
```

**Related Commands**

<b>clear configure crypto isakmp</b>	Clears all the ISAKMP configuration.
<b>clear configure crypto isakmp policy</b>	Clears all ISAKMP policy configuration.
<b>clear crypto isakmp sa</b>	Clears the IKE runtime SA database.
<b>show running-config crypto isakmp</b>	Displays all the active configuration.

# 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 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

<b>all 0</b>	Sets the limit for all resources as unlimited.
<i>number</i> [%]	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 <b>0</b> 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.
<b>rate</b>	Specifies that you want to set the rate per second for a resource. See <a href="#">Table 18-1</a> for resources for which you can set the rate per second.
<i>resource_name</i>	Specifies the resource name for which you want to set a limit. This limit overrides the limit set for <b>all</b> .

## 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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 security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the 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 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	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit <sup>1</sup>	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 <i>Cisco Security Appliance Command Line Configuration Guide</i> 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 security appliance.
asdm	Concurrent	1 minimum 5 maximum	32	ASDM management sessions. <b>Note</b> 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
<b>class</b>	Creates a resource class.
<b>context</b>	Configures a security context.
<b>member</b>	Assigns a context to a resource class.
<b>show resource allocation</b>	Shows how you allocated resources across classes.
<b>show resource types</b>	Shows the resource types for which you can set limits.

# Imfactor

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

**Imfactor** *value*

**no Imfactor**

Syntax Description	<i>value</i>
	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:
---------------	---

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

Command History	Release	Modification
	7.1(1)	This command was introduced.

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

Setting the Imfactor 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 Imfactor of 30:
----------	---

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

Related Commands	
------------------	--

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
```

<b>Related Commands</b>	<b>Commands</b>	<b>Description</b>
	<b>class</b>	Identifies a class map name in the policy map.
	<b>class-map type inspect</b>	Creates an inspection class map to match traffic specific to an application.
	<b>policy-map</b>	Creates a Layer 3/4 policy map.
	<b>policy-map type inspect</b>	Defines special actions for application inspection.
	<b>show running-config policy-map</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>router ospf</b>	Enters router configuration mode.
<b>show ospf</b>	Displays general information about the OSPF routing processes.

