l2 – lof

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.

Command Default

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **l2tp tunnel hello** command enables the ASA to detect problems with the physical layer of the L2TP connection. The default is 60 secs. With the default setting in place, you can expect the L2TP tunnel to disconnect after 180 seconds. If you configure it to a lower value, connections that are experiencing problems are disconnected earlier. The maximum retry of L2TP is 3.

Examples

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

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

Related Commands

Command	Description
show vpn-sessiondb detail 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.

lacp max-bundle

To specify the maximum number of active interfaces allowed in the EtherChannel channel group, use the **lacp max-bundle** command in interface configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp max-bundle *number*
no lacp max-bundle

Syntax Description

number	Specifies the maximum number of active interfaces allowed in the channel group, between 1 and 8; for 9.2(1) and later, the maximum is rasied to 16. If your switch does not support 16 active interfaces, be sure to set this command to 8 or fewer.

Command Default

(9.1 and earlier) The default is 8.

(9.2(1) and later) The default is 16.

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
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.2(1)	The number of active interfaces was raised from 8 to 16.

Usage Guidelines

Enter this command for a port-channel interface. The maximum number of active interfaces per channel group is eight; to decrease the number, use this command.

Examples

The following example sets the maximum number of interfaces in the EtherChannel to four:

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

lacp port-priority

To set the priority for a physical interface in an EtherChannel, use the **lacp port-priority** command in interface configuration mode. To set the priority to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp port-priority *number*
no lacp port-priority

Syntax Description

number	Sets the priority between 1 and 65535. The higher the number, the lower the priority.

Command Default

The default is 32768.

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
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

Enter this command for a physical interface. The ASA uses this setting to decide which interfaces are active and which are standby if you assign more interfaces than can be used. If the port priority setting is the same for all interfaces, then the priority is determined by the interface ID (slot/port). The lowest interface ID is the highest priority. For example, GigabitEthernet 0/0 is a higher priority than GigabitEthernet 0/1.

If you want to prioritize an interface to be active even though it has a higher interface ID, then set this command to have a lower value. For example, to make GigabitEthernet 1/3 active before GigabitEthernet 0/7, then make the **lacp port-priority** value be 12345 on the 1/3 interface vs. the default 32768 on the 0/7 interface.

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. See the **lacp system-priority** command.

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group.

Examples

The following example sets a lower port priority for GigabitEthernet 0/2 so it will be used as part of the EtherChannel ahead of GigabitEthernet 0/0 and 0/1:

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

lacp rate

To sets the rate at which the interface receives LACP data units for a physical interface in an EtherChannel, use the **lacp rate** command in interface configuration mode. To set the rate to the default, use the **no** form of this command.

Note Supported on the Secure Firewall 3100/4200 only.

lacp rate { **normal** | **fast** }
no lacp rate

Syntax Description

normal	Sets the rate to receive LACP data units to once every 30 seconds. Normal is also known as slow.
fast	Sets the rate to receive LACP data units to once every second.

Command Default

The default is normal.

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
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

When you set the rate (normal or fast), the device requests that rate from the connecting switch. In return, the device will send at the rate requested by the connecting switch. We recommend that you set the same rate on both sides.

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group.

Examples

The following example sets the rate to fast on two interfaces in an EtherChannel 1:

```
ciscoasa(config)# interface Ethernet1/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
ciscoasa(config-if)# interface Ethernet1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# lacp rate fast
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.

lacp system-priority

For EtherChannels, to set the LACP system priority globally for the ASA, use the **lacp system-priority** command in global configuration mode. To set the value to the default, use the **no** form of this command.

Note Supported on ASA hardware models and the ISA 3000 only.

lacp system-priority *number*
no lacp system-priority

Syntax Description

number	Sets the LACP system priority, from 1 to 65535. The default is 32768. The higher the number, the lower the priority. This command is global for the ASA.

Command Default

The default is 32768.

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	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

If the device at the other end of the EtherChannel has conflicting port priorities, the system priority is used to determine which port priorities to use. For interface priorities within an EtherChannel, see the **lacp port-priority** command.

Examples

The following example sets the system priority to be higher than the default (a lower number):

```
ciscoasa(config)# lacp system-priority 12345
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.

Command	Description
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

ldap-attribute-map

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.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

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 configuration 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 configuration 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:

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

Command Default

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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

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.

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

Command Default

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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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.

Command Default

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	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(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.

Command Default

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:

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

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

The **ldap-group-base-dn** command applies only to Active Directory servers using LDAP, and specifies an Active Directory hierarchy 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:

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

Related Commands

Command	Description
group-search-timeout	Adjusts the time the ASA 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 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

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.

Command Default

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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

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 ASAestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The ASA 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 ASA. 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.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
```

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

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

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.

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

Command Default

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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

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.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-naming-attribute cn
ciscoasa
(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 ASA 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** | **reference-identity** *ref_id_name*]

no ldap-over-ssl [**enable** | **reference-identity** *ref_id_name*]

Syntax Description

enable	Specifies that SSL secures a connection to an LDAP server.
reference-identity *ref_id_name*	Specifies reference-identity name to validate LDAP server identity.

Command Default

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
9.18(1)	This command was enhanced to validate the LDAP server identity.

Usage Guidelines

Use this command to specify that SSL secures a connection between the ASA 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 ASA and the LDAP server named ldapsvr1 at IP address 10.10.0.1. They also configure the plain SASL authentication mechanism.

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

To validate the LDAP server identity by specifying the reference identity name, use **reference-identity** *ref_id_name*. A reference-identity object is created using **crypto ca reference-identity refidname** with a matching criteria. When you configure reference-identity under ldap aaa-server configuration, ASA tries to find a hostname match with ldap server certificate. Failure to resolve the host or when no match is found, the connection is terminated with an error message.

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
  enable              Require an SSL connection to the LDAP server
  reference-identity  Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
  WORD < 65 char  Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
  <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

The show running-config aaa server displays the configured reference-identity name as one of the options:

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

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.
ssl-client-certificate	Specifies the certificate that the ASA should present to the LDAP server as the client certificate when using LDAPS.
crypto ca reference-identity refidname	To configure a reference-identity object.

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

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

Command Default

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 configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

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.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
```

```
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa
(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.

Command Default

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	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

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 CLI 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”:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(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 ASA before connecting.

license

To configure the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes, use the **license** command in scansafe general-options configuration mode. To remove the license, use the **no** form of this command.

license*hex_key*
no license [*hex_key*]

Syntax Description

hex_key	Specifies the authentication key as a 16-byte hexadecimal number.

Command Default

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	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Each ASA must use an authentication key that you obtain from Cloud Web Security. The authentication key lets Cloud Web Security identify the company associated with web requests and ensures that the ASA is associated with valid customer.

You can use one of two types of authentication keys for your ASA: the company key or the group key.

Company Authentication Key

A Company authentication key can be used on multiple ASAs within the same company. This key simply enables the Cloud Web Security service for your ASAs. The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter. For more information, see the Cloud Web Security documentation:
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html .

Group Authentication Key

A Group authentication key is a special key unique to each ASA that performs two functions:

- Enables the Cloud Web Security service for one ASA.
- Identifies all traffic from the ASA so you can create ScanCenter policy per ASA.

The administrator generates this key in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp); you have the opportunity to e-mail the key for later use. You cannot look up this key later in ScanCenter; only the last 4 digits are shown in ScanCenter. For more information, see the Cloud Web Security documentation: http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html .

Examples

The following example configures a primary server only:

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[s] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.

Command	Description
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

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 ASAs by configuring one of the ASAs 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 must 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:

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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 ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.

2. Decide which ASAs 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 ASA as a shared licensing backup server. You can only specify one backup server.

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

1. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
2. When you configure the ASA 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.

1. The shared licensing server responds with information about how often the participant should poll the server.
2. 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.
3. 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.

1. 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.
2. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
3. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The ASA 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:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(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:

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(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.

Command	Description
license-server address	Identifies the shared licensing server IP address and shared secret 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 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:

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

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

Command	Description
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:

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(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 ASAs by configuring one of the ASAs 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:

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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 ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which ASAs 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 ASA as a shared licensing backup server. You can only specify one backup server.

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

1. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
2. When you configure the ASA 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.

1. The shared licensing server responds with information about how often the participant should poll the server.
2. 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.
3. 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.

1. 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.
2. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
3. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The ASA 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:

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

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

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

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

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

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

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

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

Related Commands

Command	Description
activation-key	Enters a license activation key.

Command	Description
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 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.

license smart

To set the smart licensing entitlement request, use the **license smart** command in global configuration mode. To remove the entitlement and unlicense your device, use the **no** form of this command.

Note This feature is supported on the ASA virtual and Chassis only.

license smart
no license smart

Syntax Description

This command has no arguments or keywords.

Command Default

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	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.4(1.152)	Support for the Firepower 9300 was added.
9.6(1)	Support for the Firepower 4100 series was added.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

This command enters license smart configuration mode, where you can set the feature tier and other license entitlements. For the ASA virtual, when you request the entitlements for the first time, you must exit license smart configuration mode for your changes to take effect.

Examples

The following example sets the feature tier to standard, and the throughput level to 2G:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart deregister

To deregister the device from the Cisco License Authority for smart licensing, use the **license smart deregister** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart deregister

Syntax Description

This command has no arguments or keywords.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

Deregistering the ASA removes the ASA from your account. All license entitlements and certificates on the ASA are removed. You might want to deregister to free up a license for a new ASA. This command causes the ASA to reload.

Examples

The following example deregisters the device:

```
ciscoasa# license smart deregister
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.

Command	Description
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart register

To register the device with the Cisco License Authority for smart licensing, use the **license smart register** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart register idtoken *id_token* [**force**]

Syntax Description

idtoken *id_token*	In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this ASA.
force	Registers an ASA that is already registered, but that might be out of sync with the License Authority.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

When you register the ASA, the License Authority issues an ID certificate for communication between the ASA and the License Authority. It also assigns the ASA to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the ASA if the ID certificate expires because of a communication problem, for example.

Examples

The following example registers with an registration token:

```
ciscoasa# license smart register idtoken
YjE3Njc5MzYtMGQzMi00OTA4LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQkdYRmZ1NINONGlvRnBHUFpjcm02WlB4TU4w%0Ac2NhMD0%3D%0A
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart renew

To renew the registration or license entitlement authorization for smart licensing, use the **license smart renew** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual and Firepower 2100 only.

license smart renew { **id** | **auth** }

Syntax Description

id	Renews the device registration.
auth	Renews the license entitlement.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for internet access, or if you make any licensing changes in the Smart Software Manager, for example.

Examples

The following example renews both the registration and license authorization:

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

license smart reservation

To enable permanent license reservation, use the **license smart reservation** command in global configuration mode. To disable permanent license reservation, use the **no** form of this command.

license smart reservation
no license smart reservation

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled 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
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory). The permanent license enables all features to their maximum levels.

For the ASA virtual, when you enter the **license smart reservation** command, the following commands are removed:

```
license smart
feature tier standard
throughput level {100M | 1G | 2G}
```

To use regular smart licensing, use the **no** form of this command, and re-enter the above commands. Other Smart Call Home configuration remains intact but unused, so you do not need to re-enter those commands.

For Chassis, you must enter the **license smart**/**feature** commands for any non-default licenses; for example, for the context license. These commands are required so the ASA knows to allow configuration of the feature.

Note For permanent license reservation, you must return the license before you decommission the ASA. If you do not officially return the license, the license remains in a used state and cannot be reused for a new ASA. See the **license smart reservation return** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation cancel

To cancel a permanent license reservation request if you have not yet entered the code in the Smart Software Manager, use the **license smart reservation cancel** command in privileged EXEC mode.

license smart reservation cancel

Note This feature applies only to the ASA virtual and the Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

If you requested a license code to enter in the Smart Software Manager using the **license smart reservation request universal** command, and have not yet entered this code into the Smart Software Manager, you can cancel the request using the **license smart reservation cancel** command.

If you disable permanent license reservation (**no license smart reservation**), then any pending requests are canceled.

If you already entered the code into the Smart Software Manager, then you must finish applying the license to the ASA, after which point you can return the license using the **license smart reservation return** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then cancels the request:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
```

```
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation install

To enter a permanent license reservation authorization code received from the Smart Software Manager, use the **license smart reservation install** command in privileged EXEC mode.

license smart reservation install *code*

Note This feature applies only to the ASA virtual and the Firepower 2100.

Syntax Description

code	The permanent license reservation authorization code received from the Smart Software Manager.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager (https://software.cisco.com/#SmartLicensing-Inventory). Request a code to enter into the Smart Software Manager using the **license smart reservation request universal** command. When you enter the code into the Smart Software Manager, copy the resulting authorization code and enter it on the ASA using the **license smart reservation install** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation universal

To request the license code to enter in the Smart Software Manager, use the **license smart reservation universal** command in privileged EXEC mode.

license smart reservation universal

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager. Request a code to enter into the Smart Software Manager using the **license smart reservation request universal** command.

The ASA virtual deployment determines which license (ASAv5/ASAv10/ASAv30) is requested.

If you re-enter this command, then the same code is displayed, even after a reload. If you have not yet entered this code into the Smart Software Manager and want to cancel the request, enter the **license smart reservation cancel** command.

If you disable permanent license reservation, then any pending requests are canceled. If you already entered the code into the Smart Software Manager, then you must complete this procedure to apply the license to the ASA, after which point you can return the license if desired. See the **license smart reservation return** command.

To request the authorization code, go to the Smart Software Manager Inventory screen (https://software.cisco.com/#SmartLicensing-Inventory), and click the **Licenses** tab. The **Licenses** tab displays all existing licenses related to your account, both regular and permanent. Click **License Reservation**, and type the ASA code into the box. Click **Reserve License**. The Smart Software Manager generates an authorization code. You can download the code or copy it to the clipboard. At this point, the license is now in use according to the Smart Software Manager.

If you do not see the **License Reservation** button, then your account is not authorized for permanent license reservation. In this case, you should disable permanent license reservation and re-enter the regular smart license commands.

Enter the authorization code on the ASA using the **license smart reservation install** command.

Examples

The following example enables permanent license reservation, requests the license code to enter in the Smart Software Manager, and then installs the authorization code you received from the Smart Software Manager:

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

license smart reservation return

To generate a return code to return the license to the Smart Software Manager, use the **license smart reservation return** command in privileged EXEC mode.

license smart reservation return

Note This feature applies only to the ASA virtual and Firepower 2100.

Syntax Description

This command has no arguments or keywords.

Command Default

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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(2.200)	We introduced this command for ASA virtual support.
9.8(2)	Support for the Firepower 2100 series was added.

Usage Guidelines

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager. If you no longer need a permanent license (for example, you are retiring an ASA or changing the ASA virtual model level so it needs a new license), you must officially return the license to the Smart Software Manager. If you do not return the license, then the license stays in a used state and cannot easily be freed up for use elsewhere.

When you enter the **license smart reservation return** command, the ASA immediately becomes unlicensed and moves to the Evaluation state. If you need to view this code again, re-enter this command. Note that if you request a new permanent license (**license smart reservation request universal**) or change the ASA virtual model level (by powering down and changing the vCPUs/RAM), then you cannot re-display this code. Be sure to capture the code to complete the return.

Before you enter the code in the Smart Software Manager, view the ASA universal device identifier (UDI) using the **show license udi** command so you can find this ASA instance in the Smart Software Manager. Go to the Smart Software Manager Inventory screen (https://software.cisco.com/#SmartLicensing-Inventory), and click the **Product Instances** tab. The **Product Instances** tab displays all licensed products by the UDI.

Find the ASA virtual you want to unlicense, choose **Actions** > **Remove**, and type the ASA return code into the box. Click **Remove Product Instance**. The permanent license is returned to the available pool.

Examples

The following example generates the return code on the ASA virtual, and views the ASA virtual UDI:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

Related Commands

Command	Description
license smart reservation	Enables permanent license reservation.
license smart reservation cancel	Cancels the permanent license request if you have not entered the code in the Smart Software Manager.
license smart reservation install	Enters the authorization code.
license smart reservation request universal	Requests the license code to enter in the Smart Software Manager.
license smart reservation return	Returns the license to the Smart Software Manager.

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*
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 5 to 30 years. The default lifetime value is 15 years. For all the issued user certificates, the valid range is from one day to four years. The default lifetime value is 2 years. 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.

Command Default

The default lifetimes are:

- CA certificate—15 years
- Issued certificates— Two years
- CRL—Six hours

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
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.12(1)	The allowed values for lifetime ca-certificate is changed to 5 to 30 years with a default of 15 years. The allowed values for lifetime certificate is changed to 1 day to 4 years with a default of 2 years.

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.

The **lifetime ca-certificate** command takes effect when the local CA server certificate is first generated (that is, when you initially configure the local CA server and issue the **no shutdown** command). When the CA certificate expires, the configured lifetime value is used to generate the new CA certificate. You cannot change the lifetime value for existing CA certificates.

Examples

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

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

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

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

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point (CDP) to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode 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.

lifetime (ikev2 policy mode)

To specify the encryption algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the encryption command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

lifetime { { **seconds** *seconds* } | **none** }

Syntax Description

seconds	The lifetime in seconds, from 120 to 2,147,483,647 seconds. The default is 86,400 seconds (24 hours).

Command Default

The default is 86,400 seconds (24 hours).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **lifetime** command to set the SA lifetime.

The lifetime sets the interval for IKEv2 SA rekeys. Using the none keyword disables rekeying the SA. However, the Secure Client can still rekey the SA.

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	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.

Examples

The following example enters IKEv2 policy configuration mode and sets the lifetime to 43,200 seconds (12 hours):

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.

Command	Description
prf	Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections.

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

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

Syntax Description

all	Sets the limit for all resources.
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, or for VPN resource types, to set the limit to none. 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 1: Resource Names and Limits 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**.

Command Default

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

For most resources, the default class provides unlimited access to resources for all contexts, except for the following limits:

- Telnet sessions—5 sessions. (The maximum per context.)
- SSH sessions—5 sessions. (The maximum per context.)
- ASDM sessions—5 sessions. (The maximum per context.)
- IPsec sessions—5 sessions. (The maximum per context.)
- MAC addresses—(varies per model). (The maximum per context.)
- AnyConnect peers—0 sessions. (You must manually configure the class to allow any AnyConnect peers.)
- VPN site-to-site tunnels—0 sessions. (You must manually configure the class to allow any VPN sessions.)

Note If you also set the **quota management-session** command within a context to set the maximum administrative sessions (SSH, etc.), then the lower value will be used.

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	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	A new resource type, **routes**, was created to set the maximum number of routing table entries in each context. New resource types, **vpn other** and **vpn burst other**, were created to set the maximum number of site-to-site VPN tunnels in each context.
9.5(2)	New resource types, **vpn anyconnect** and **vpn burst anyconnect**, were created to set the maximum number of AnyConnect VPN peers in each context.
9.6(2)	New resource type, **storage**, was created to set the maximum storage.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced; the only exception is VPN resources, which are disabled by default. If you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context. For VPN resources, you must configure resource management to allow any VPN tunnels.

Table 1: Resource Names and Limits lists the resource types and the limits. See also the **show resource types** command.

Table 1: Resource Names and Limits

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
asdm	Concurrent	1 minimum 5 maximum	200	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 200 ASDM sessions represents a limit of 400 HTTPS sessions.

Resource Name	**Rate or Concurrent**	**Minimum and Maximum Number per Context**	**System Limit**[1]	**Description**
conns	Concurrent or Rate	N/A	Concurrent connections: See the CLI configuration guide 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.
hosts	Concurrent	N/A	N/A	Hosts that can connect through the ASA.
inspects	Rate	N/A	N/A	Application inspections.
mac-addresses	Concurrent	N/A	(varies per model)	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
routes	Concurrent	N/A	N/A	Dynamic routes.
ssh	Concurrent	1 minimum 5 maximum	100	SSH sessions.
storage	MB	The maximum depends on your specified flash memory drive	The maximum depends on your specified flash memory drive	Storage limit of context directory in MB. Specify the drive using the **storage-url** command.
syslogs	Rate	N/A	N/A	System log messages.
telnet	Concurrent	1 minimum 5 maximum	100	Telnet sessions.
vpn burst anyconnect	Concurrent	N/A	The AnyConnect Premium Peers for your model minus the sum of the sessions assigned to all contexts for vpn anyconnect.	The number of AnyConnect sessions allowed beyond the amount assigned to a context with **vpn anyconnect**. For example, if your model supports 5000 peers, and you assign 4000 peers across all contexts with **vpn anyconnect**, then the remaining 1000 sessions are available for **vpn burst anyconnect**. Unlike **vpn anyconnect**, which guarantees the sessions to the context, **vpn burst anyconnect** can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.
vpn anyconnect	Concurrent	N/A	See the "Supported Feature Licenses Per Model" section in the CLI configuration guide for the AnyConnect VPN peers available for your model.	AnyConnect peers. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The peers you assign for this resource are guaranteed to the context.

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
vpn burst other	Concurrent	N/A	The Other VPN session amount for your model minus the sum of the sessions assigned to all contexts for **vpn other**.	The number of site-to-site VPN sessions allowed beyond the amount assigned to a context with **vpn other**. For example, if your model supports 5000 sessions, and you assign 4000 sessions across all contexts with **vpn other**, then the remaining 1000 sessions are available for **vpn burst other**. Unlike **vpn other**, which guarantees the sessions to the context, **vpn burst other** can be oversubscribed; the burst pool is available to all contexts on a first-come, first-served basis.
vpn other	Concurrent	N/A	See the "Supported Feature Licenses Per Model" section in the CLI configuration guide for the Other VPN sessions available for your model.	Site-to-site VPN sessions. You cannot oversubscribe this resource; all context assignments combined cannot exceed the model limit. The sessions you assign for this resource are guaranteed to the context.
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:

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

All other resources remain at unlimited.

To add a class called gold, enter the following commands:

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

```
ciscoasa(config-class)#
limit-resource xlates 36000
ciscoasa(config-class)#
limit-resource routes 700
```

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*
nolmfactor

Syntax Description

value	An integer in the range of 0 to 100.

Command Default

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 configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The ASA 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 ASA 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:

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(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 size of an object to cache.

load-monitor

To configure cluster traffic load monitoring, use the **load-monitor** command in cluster configuration mode. To disable this feature, use the **no** form of this command.

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]
no load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

Syntax Description

frequency *seconds*	(Optional) Sets the time in seconds between monitoring messages, between 10 and 360 seconds. The default is 20 seconds.
intervals *intervals*	(Optional) Sets the number of intervals for which the ASA maintains data, between 1 and 60. The default is 30.

Command Default

This command is enabled by default. The default frequency is 20 seconds. The default interval is 30.

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
Cluster configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

You can monitor the traffic load for cluster members, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the unit if the remaining units can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default. For example, for inter-chassis clustering on the Firepower 9300 with 3 security modules in each chassis, if 2 security modules in a chassis leave the cluster, then the same amount of traffic to the chassis will be sent to the remaining module and potentially overwhelm it. You can periodically monitor the traffic load. If the load is too high, you can choose to manually disable clustering on the unit.

Use the **show cluster info load-monitor** command to view the traffic load.

Examples

The following example sets the frequency to 50 seconds, and the interval to 25:

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

Related Commands

Command	Description
cluster	Enters cluster configuration mode

local-base-url

(Optional) Configures the local base URL of the SAML service provider for VPN authentication. In a DNS load balancing cluster, when you configure SAML authentication on ASAs, you can specify this URL to uniquely resolve to the device on which the configuration is applied.

To disable this feature, use the **no** form of this command

local base-url { **url** }
no local base-url

Syntax Description

url	Local base URL of the SAML service provider for VPN authentication.

Command Default

None.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(3)	This command was added.
9.19(1)5	This command was added.

Usage Guidelines

You must use this command in conjunction with the **base-url** command.

Examples

The following example sets up a local base-url:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp https://idp.com/<app-specific>
ciscoasa(config-webvpn-saml-idp)# base url https://asa-dns-group.vpn.customer.com
ciscoasa(config-webvpn-saml-idp)# local-base-url https://this-asa.vpn.customer.com
```

Related Commands

Command	Description
signature	Enable or disable signature in SAML request. By default, the signature is disabled.
timeout	Configures the SAML IdP timeout.
trustpoint	Configures the trustpoint in saml-idp sub-mode.

Command	Description
url	Configures the SAML IdP URL.
base-url	Configures the base URL of the SAML service provider for VPN authentication.

local-domain-bypass

To configure local domains for which DNS requests should bypass Cisco Umbrella, use the **local-domain-bypass** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }
no local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }

Syntax Description

regular_expression	A regular expression that identifies the local domain to bypass. This can be as simple as the local domain, for example, example.com. The expression can be up to 100 characters. If you use this option, you can enter the **local-domain-bypass** command multiple times to define more than one local domain.
regex class *regex_classmap*	The name of the regular expression class that defines the local domain names to bypass. Any DNS requests for fully-qualified domain names that match the regular expressions in the class are sent directly to the configured DNS servers, not to the Umbrella servers.

Command Default

The default is that DNS requests for all domains are sent to Cisco Umbrella.

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
Umbrella configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

Following are the guidelines for using this command:

- You can enter this command multiple times to define regular expressions for domain names directly.
- You can enter this command only once when using a regular expression class. However, you can combine both a single regular expression class version of the command with multiple instances where you use a regular expression directly.

Examples

The following example defines example.com as the local domain to bypass.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass example.com
```

The following example creates a regular expression to match example.com, which would match any fully-qualified domain name on *example.com. Then, the example creates the required regular expression class map and uses it as the local domain bypass for Umbrella.

```
ciscoasa(config)# regex example-com example.com

ciscoasa(config)# class-map type regex match-any umbrella-bypass

ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

Related Commands

Commands	Description
umbrella-global	Configures the Cisco Umbrella global parameters.

local-unit

To provide a name for this cluster member, use the **local-unit** command in cluster group configuration mode. To remove the name, use the **no** form of this command.

local-unit *unit_name*
no local-unit [*unit_name*]

Syntax Description

unit_name	Names this member of the cluster with a unique ASCII string from 1 to 38 characters.

Command Default

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
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Each unit must have a unique name. A unit with a duplicated name will be not be allowed in the cluster.

Examples

The following example names this unit as unit1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.

Command	Description
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

location-logging

To have GTP inspection log the location and change of location for mobile stations, use the **location-logging** command in GTP inspection policy map parameters configuration mode. Use the **no** form of this command to disable location logging.

location-logging [**cell-id**]
no location-logging [**cell-id**]

Syntax Description

cell-id	Whether to include the cell ID where the user currently is registered. The cell ID is extracted from the Cell Global Identification (CGI) or E-UTRAN Cell Global Identifier (ECGI).

Command Default

By default, location logging 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
Parameters configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

You can use GTP inspection to track location changes for mobile stations. Tracking location changes might help you identify fraudulent roaming charges, for example, if you see a mobile station move from one location to another within an unlikely time window, such as moving from a cell in the United States to one in Europe within 30 minutes.

When you enable location logging, the system generates syslog messages for new or changed locations for each International Mobile Subscriber Identity (IMSI):

- 324010 indicates the creation of a new PDP context, and includes the Mobile Country Code (MCC), Mobile Network Code (MNC), the information elements, and optionally the cell ID where the user currently is registered. The cell ID is extracted from the Cell Global Identification (CGI) or E-UTRAN Cell Global Identifier (ECGI).
- 324011 indicates that the IMSI has moved from the one stored during the PDP context creation. The message shows the previous and current MCC/MNC and optionally, cell ID.

By default, syslog messages do not include timestamp information. If you plan to analyze these messages to identify improbable roaming, you must also enable timestamps. Timestamp logging is not part of the GTP inspection map. Use the **logging timestamp** command.

Examples

The following example adds the timestamp to syslog messages and then enables location logging with the cell ID.

```
ciscoasa(config)# logging timestamp

ciscoasa(config)# policy-map type inspect gtp gtp-map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# location-logging cell-id
```

Related Commands

Commands	Description
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.
show service-policy inspect gtp	Displays the GTP configuration and statistics.