da – dg

database path

To specify a path or location for the local CA server database, use the **database** command in ca server configuration mode. To reset the path to flash memory, the default setting, use the **no** form of this command.

[**no**] **database path** *mount-name directory-path*

Syntax Description

directory-path	Specifies the path to a directory on the mount point where the CA files are stored.
mount-name	Specifies the mount name.

Command Default

By default, the CA server database is stored in flash memory.

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.

Usage Guidelines

The local CA files stored in the database include the certificate database, user database files, temporary PKCS12 files, and the current CRL file. The *mount-name* argument is the same as the *name* argument for the **mount** command that is used to specify a file system for the ASA.

Note These CA files are internal, stored files and should not be modified.

Examples

The following example defines the mount point for the CA database as cifs_share and the database files directory on the mount point as ca_dir/files_dir:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# database path cifs_share ca_dir/files_dir/
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows the user to configure and manage a local CA.
crypto ca server user-db write	Writes the user information configured in the local CA database to disk.
debug crypto ca server	Shows debugging messages when the user configures the local CA server.
mount	Makes the Common Internet File System (CIFS) and/or File Transfer Protocol file systems (FTPFS) accessible to the ASA.
show crypto ca server	Displays the characteristics of the CA configuration on the ASA.
show crypto ca server cert-db	Displays the certificates issued by the CA server.

data-plane quick-reload

To quickly reload the data-plane and resynchronize with adjacent processes, use the **data-plane quick-reload** command. To remove the quick reload option, use the **no** form of this command.

[**no**] **data-plane quick-reload**

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the quick reload of the data plane is enabled.

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 Mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.20(2)	This command was added.

Usage Guidelines

When you want to reload the data plane process rather than a reboot of the device, you can use the **data-plane quick-reload** command. When data plane quick reload is enabled, it restarts the data plane and also the following processes:

- SNORT2/SNORT3/PDTS.
- SNMPD—Restarted if already running
- SYSLOGD—Restarted if already running
- LICENCE SMART AGENT—Restarted if already running
- OFFLOAD APP—Restarted and all flows are flushed
- SERVICE MANAGER—Re-registers with service manager

However, when lina crash occurs during a boot up, the device aborts the quick restart and instead follows the normal device reload/reboot sequence. This exception is done to avoid continuous looping of the quick restart process.

Related Commands

Command	Description
show data-plane quick-reload status	Displays the status of the reload of the data plan.

ddns

To specify a Dynamic DNS (DDNS) update method type, use the **ddns** command in ddns-update-method mode. To remove an update method type from the running configuration, use the **no** form of this command.

ddns [**both**]
no ddns [**both**]

Syntax Description

both	(Optional) Specifies updates to both the DNS A and PTR resource records (RRs).

Command Default

Update only the DNS A RRs.

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
Ddns-update-method	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mappings are contained in two types of RRs:

- The A resource record contains domain name-to-IP address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.

When issued in ddns-update-method configuration mode, the **ddns** command defines whether the update is just to a DNS A RR, or to both DNS A and PTR RR types.

Examples

The following example configures updates to both the DNS A and PTR RRs for the DDNS update method named ddns-2:

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

Related Commands

Command	Description
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update

To associate a dynamic DNS (DDNS) update method with an ASA interface or an update hostname, use the **ddns update** command in interface configuration mode. To remove the association between the DDNS update method and the interface or the hostname from the running configuration, use the **no** form of this command.

ddns update [*method-name* | **hostname** *hostname*]
no ddns update [*method-name* | **hostname** *hostname*]

Syntax Description

hostname	Specifies that the next term in the command string is a hostname.
hostname	Specifies a hostname to be used for updates.
method-name	Specifies a method name for association with the interface being configured.

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
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

After defining a DDNS update method, you must associate it with an ASA interface to trigger DDNS updates.

A hostname could be a Fully Qualified Domain Name (FQDN) or just a hostname. If just a hostname, the ASA appends a domain name to the hostname to create a FQDN.

Examples

The following example associates the interface GigabitEthernet0/2 with the DDNS update method named ddns-2 and the hostname hostname1.example.com:

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.

Command	Description
ddns update method	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update method

To create a method for dynamically updating DNS resource records (RRs), use the **ddns update method** command in global configuration mode. To remove a dynamic DNS (DDNS) update method from the running configuration, use the **no** form of this command.

ddns update method *name* [**web** { **reference-identity** *name* | **update-type** { **ipv4** | **ipv6** } | **update-url** *url* }]
no ddns update method *name*

Syntax Description

name	Specifies the name of a method for dynamically updating DNS records.
reference-identity	Specifies the reference-identity name to validate server identity.
update-type	Specifies the type of update to be sent—ipv4 or ipv6.
update-url	Specifies the update URL for DDNS update.

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	—

Command History

Release	Modification
7.2(1)	This command was added.
9.18(1)	The option to specify the reference identity name that is configured to match server certificate identity was added.

Usage Guidelines

DDNS updates the name-to-address and address-to-name mapping maintained by DNS. The update method configured by the **ddns update method** command determines what and how often DDNS updates are performed. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the ASA supports the IETF method in this release.

Name and address mapping is contained in two types of resource records (RRs):

- The A resource record contains domain name-to IP-address mapping.
- The PTR resource record contains IP address-to-domain name mapping.

DDNS updates can be used to maintain consistent information between the DNS A and PTR RR types.

Note Before the **ddns update method** command will work, you must configure a reachable default DNS server using the **dns** command with domain lookup enabled on the interface.

Examples

The following example configures the DDNS update method named ddns-2:

```
ciscoasa(config)# ddns update method ddns-2
```

To validate connecting to DDNS server with reference-identity object, use **reference-identity** *ref_id_name*. A reference-identity object is created using **crypto ca reference-identity refidname** with a matching criteria. When reference-identity is configured, while attempting to connect to ddns server, ASA validates server certificate identity with a matching hostname. Failure to resolve the host or when no match is found, the connection is terminated with an error message.

```
asa(config-aaa-server-host)# ddns update method tempddns
asa(DDNS-update-method)# web ?

dynupd-method mode commands/options:
  reference-identity  Enter Reference-identity name to validate server identity
  update-type         Configure the type of update to be sent
  update-url          Configure Update URL for DDNS update
```

The configured reference-identity is displayed in the show running-config command:

```
asa(DDNS-update-method)# web reference-identity dyndns
asa(DDNS-update-method)# show running-config ddns
ddns update method tempddns
web update-url
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
web update-type ipv4
web reference-identity dyndns
interval maximum 0 0 2 0
!
asa(DDNS-update-method)#

asa(DDNS-update-method)# sh ddns update method
Dynamic DNS Update Method: dyndns
Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
  Update type configured: ipv4
  Configured reference-identity name: dyndns
  Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
asa(DDNS-update-method)#
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a DDNS update method with an ASA interface or a DDNS update hostname.

Command	Description
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

debug

To show debugging messages for a given feature, use the **debug** command in privileged EXEC mode. To disable the display of debug messages, use the **no** form of this command.

debug feature [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

level	(Optional) Specifies the debugging level. The level may not be available for all features.
feature	Specifies the feature for which you want to enable debugging. To see available features, use the **debug ?** command for CLI help.
subfeature	(Optional) Depending on the feature, you can enable debug messages for one or more subfeatures.

Command Default

The default debugging level is 1.

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	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	The **debug crypto ca** command was modified to reduce the options and to restrict the debugging level to 14.
9.18(1)	This command was modified to include the debug for path monitoring.
9.20(1)	This command was modified to include the debug for EIGRP IPv6.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

From version 9.13(1), the options to the **debug crypto ca** command, namely **debug crypto ca transactions** and **debug crypto ca messages** are consolidated to provide all applicable content into the **debug crypto ca** command itself. Also, the number of available debugging levels were reduced to 14.

Examples

The following is sample output from the **debug aaa internal** command:

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

The following is the modified **debug crypto ca** command:

```
(config)# debug crypto ca ?
exec mode commands/options:
  <1-14>                   Specify an optional debug level (default is 1)
  cluster                  debug PKI cluster
  cmp                      debug the CMP transactions
  periodic-authentication  debug PKI peroidic authentication
  <cr>
```

default (crl configure)

To return all CRL parameters to their system default values, use the **default** command in crl configure configuration mode.

default

Syntax Description

This command has no arguments or keywords.

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
Crl configure configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

Examples

The following example enters ca-crl configuration mode and returns CRL command values to their defaults:

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

Related Commands

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

default (interface)

To return an interface command to its system default value, use the **default** command in interface configuration mode.

default*command*

Syntax Description

command Specifies the command that you want to set to the default. For example:

```
default activation key
```

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
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is a runtime command; when you enter it, it does not become part of the active configuration.

Examples

The following example enters interface configuration mode and returns the security level to its default:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

default (ipv6 router ospf)

To return an OSPFv3 parameter to its default value, use the **default** command in ipv6 router ospf configuration mode.

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Syntax Description

area	(Optional) Specifies the OSPFv3 area parameters.
auto-cost	(Optional) Specifies the OSPFv3 interface cost according to the bandwidth.
default-information	(Optional) Distributes default information.
default-metric	(Optional) Specifies the metric for a redistributed route.
discard-route	(Optional) Enables or disables discard-route installation.
distance	(Optional) Specifies the administrative distance.
distribute-list	(Optional) Filters networks in routing updates.
ignore	(Optional) Ignores a specific event.
log-adjacency-changes	(Optional) Logs changes in the adjacency state.
maximum-paths	(Optional) Forwards packets over multiple paths.
passive-interface	(Optional) Suppresses routing updates on an interface.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
router-id	(Optional) Specifies the router ID for the specified routing process.
summary-prefix	(Optional) Specifies the OSPFv3 summary prefix.
timers	(Optional) Specifies the OSPFv3 timers.

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
Router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to reset OSPFv3 parameter default values.

Examples

The following example resets OSPFv3 timer parameters to their default values:

```
ciscoasa(config-router)# d
efault timers spf
```

Related Commands

Command	Description
distance	Specifies the administrative distance for OSPFv3 routing processes.
default-information originate	Generates a default external route into an OSPFv3 routing domain.
log-adjacency-changes	Configures the router to send a syslog message when an OSPFv3 neighbor goes up or down.

default (parameters)

To define the default action for options for which specific actions are not specified during IP Options inspection, use the **default** command in parameters configuration mode. To return to system defaults, use the **no** form of this command.

default action { **allow** | **clear** }
no default action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing options not explicitly identified in the IP options inspection policy map.
clear	Remove options not explicitly identified in the IP options inspection policy map from packet headers and then allow the packets.

Command Default

By default, IP Options inspection allows the router-alert option but drops packets containing any other IP option.

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
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action clear
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

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

default (time-range)

To restore default settings for the **absolute** and **periodic** commands, use the **default** command in time-range configuration mode.

default { **absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time* }

Syntax Description

absolute	Defines an absolute time when a time range is in effect.
days-of-the-week	The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
periodic	Specifies a recurring (weekly) time range for functions that support the time range feature.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

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
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the absolute start time is reached, and are not further evaluated after the absolute end time is reached.

The time-range feature relies on the system clock of the ASA; however, the feature works best with NTP synchronization.

Examples

The following example shows how to restore the default behavior of the **absolute** keyword:

```
ciscoasa(config-time-range)# default absolute
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
periodic	Specifies a recurring (weekly) time range for functions that support the time range feature.
time-range	Defines access control to the ASA based on time.

default-acl

To specify the ACL to be used as the default ACL for NAC Framework sessions that fail posture validation, use the **default-acl** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of the command.

[**no**] **default-acl** *acl-name*

Syntax Description

acl-name	Names the access control list to be applied to the session.

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
Nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	"nac-" was removed from the command name. The command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

Each group policy points to a default ACL to be applied to hosts that match the policy and are eligible for NAC. The ASA applies the NAC default ACL before posture validation. After posture validation, the ASA replaces the default ACL with the one obtained from the Access Control Server for the remote host. It retains the default ACL if posture validation fails.

The ASA also applies the NAC default ACL if clientless authentication is enabled (which is the default setting).

Examples

The following example identifies acl-1 as the ACL to be applied before posture validation succeeds:

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

The following example inherits the ACL from the default group policy:

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
debug nac	Enables logging of NAC Framework events.
show vpn-session_summary.db	Displays the number of IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

default-domain

To set a default domain name for users of the group policy, use the **default-domain** command in group-policy configuration mode. To delete a domain name, use the **no** form of this command.

default-domain { **value** *domain-name* | **none** }
no default-domain [*domain-name*]

Syntax Description

none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.
value *domain-name*	Identifies the default domain name for the group.

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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To prevent users from inheriting a domain name, use the **default-domain none** command.

The ASA passes the default domain name to the Secure Client or the legacy VPN client (IPsec/IKEv1) to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. When there are no default domain names, users inherit the default domain name in the default group policy.

You can use only alphanumeric characters, hyphens (-), and periods (.) in default domain names.

Examples

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

Related Commands

Command	Description
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in clear text form.

default enrollment

To return all enrollment parameters to their system default values, use the **default enrollment** command in crypto ca trustpoint configuration mode.

default enrollment

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
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Invocations of this command do not become part of the active configuration.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and returns all enrollment parameters to their default values within trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

default-group-policy (imap4s, pop3s, smtps) (Deprecated)

Note The last supported release of this command was 7.5(1).

To specify the name of the group policy to use when e-mail proxy configuration does not specify a group policy, use the **default-group-policy** command in various configuration modes. To remove the attribute from the configuration, use the **no** form of this command.

default-group-policy*groupname*
nodefault-group-policy

Syntax Description

groupname	Identifies the previously configured group policy to use as the default group policy. Use the **group-policy** command to configure a group policy.

Command Default

A default group policy, named *DfltGrpPolicy*, always exists on the ASA. This **default-group-policy** command lets you substitute a group policy that you create as the default group policy e-mail proxy sessions. An alternative is to edit the DfltGrpPolicy.

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
Imap4s configuration	• Yes	—	• Yes	—	—
Pop3s configuration	• Yes	—	• Yes	—	—
Smtps configuration	• Yes	—	• Yes	—	—

Command History

Version	Modification
7.0(1)	This command was added.
7.5(2)	This command was deprecated.

Usage Guidelines

IMAP4S, POP3S, and SMTPS sessions require either a specified or a default group policy. Use this command in the applicable e-mail proxy mode.

You can edit, but not delete the system DefaultGroupPolicy. It has the following AVPs:

Attribute	Default Value
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none

Attribute	Default Value
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

Examples

The following example shows how to specify a default group policy called pop3s for POP3S:

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-webvpn)# default-group-policy pop3s
```

default-group-policy (tunnel-group general-attributes)

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

default-group-policy*group-name*
no default-group-policy *group-name*

Syntax Description

group-name	Specifies the name of the default group.

Command Default

The default group name is DfltGrpPolicy.

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
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Version	Modification
7.0(1)	This command was added.
7.1(1)	The **default-group-policy** command in webvpn configuration mode was deprecated. The **default-group-policy** command in tunnel-group general-attributes mode replaced it.

Usage Guidelines

In Version 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

The default group policy DfltGrpPolicy comes with the initial configuration of the ASA. You can apply this attribute to all tunnel group types.

Examples

The following example entered in config-general configuration mode, specifies a set of attributes for users to inherit by default for an IPsec LAN-to-LAN tunnel group named “standard-policy.” This set of commands defines the accounting server, the authentication server, the authorization server, and the address pools.

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
```

```
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-policy	Creates or edits a group policy
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel group.

default-idle-timeout

To set a default idle timeout value for WebVPN users, use the **default-idle-timeout** command in webvpn configuration mode. To remove the default idle timeout value from the configuration and reset the default, use the **no** form of this command.

default-idle-timeout*seconds*
no default-idle-timeout

Syntax Description

seconds	Specifies the number of seconds for the idle time out. The minimum is 60 seconds, maximum is 1 day (86400 seconds).

Command Default

1800 seconds (30 minutes).

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
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA uses the value you set here if there is no idle timeout defined for a user, if the value is 0, or if the value does not fall into the valid range. The default idle timeout prevents stale sessions.

We recommend that you set this command to a short time period, because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the maximum number of connections permitted is set to one (via the **vpn-simultaneous-logins** command), the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.

Examples

The following example shows how to set the default idle timeout to 1200 seconds (20 minutes):

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

Related Commands

Command	Description
vpn-simultaneous-logins	Sets the maximum number of simultaneous VPN sessions permitted.

default-information

To control the candidate default route information for the EIGRP routing process, use the **default-information** command in router eigrp configuration mode. To suppress EIGRP candidate default route information in incoming or outbound updates, use the **no** form of this command.

default-information { **in** | **out** } [*acl-name*]
no default-information { **in** | **out** }

Syntax Description

acl-name	(Optional) Specifies the named standard access list.
in	Configures EIGRP to accept exterior default routing information.
out	Configures EIGRP to advertise external routing information.

Command Default

Exterior routes are accepted and sent.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Only the **no** form of the command or **default-information** commands with an access list specified will appear in the running configuration because, by default, the candidate default routing information is accepted and sent. The **no** form of the command does not take an *acl-name* argument.

Examples

The following example disables the receipt of exterior or candidate default route information:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

default-information originate

To generate a default route into an IS-IS routing domain, use the **default-information originate** command in router isis configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]
no default-information originate [**route-map** *map-name*]

Syntax Description

route-map	(Optional) Routing process generates the default route if the route map is satisfied.
map-name	Name of the route map.

Command Default

This command 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
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If an ASA configured with this command has a route to 0.0.0.0 in the routing table, IS-IS originates an advertisement for 0.0.0.0 in its LSPs.

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the ASA generate default in its Level 1 LSPs.
- Advertise 0/0 conditionally.

With a **match ip address standard-access-list** command, you can specify one or more IP routes that must exist before the router will advertise 0/0.

Examples

The following example forces the software to generate a default external route into an IS-IS domain:

```
router isis
! ISIS routes will be distributed into IS-IS
```

```
redistribute isis 120 metric
! access list 2 is applied to outgoing routing updates
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

default-information originate (address-family)

To configure a Border Gateway Protocol (BGP) routing process to distribute a default route (network 0.0.0.0), use the default-information originate command in address-family configuration mode. To disable the advertisement of a default route, use the no form of this command.

default-informationoriginate
no default-information originate

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
Address family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The default-information originate command is used to configure a BGP routing process to advertise a default route (network 0.0.0.0). A redistribution statement must also be configured to complete this configuration or the default route will not be advertised.

The configuration of the default-information originate command in BGP is similar to the configuration of the network (BGP) command. The default-information originate command, however, requires explicit redistribution of the route 0.0.0.0. The network command requires only that the route 0.0.0.0 is present in the Interior Gateway Protocol (IGP) routing table. For this reason, the network command is preferred.

Note The default-information originate command should not be configured with the neighbor default-originate command on the same router. You should configure one or the other.

Examples

In the following example, the router is configured to redistribute a default route from OSPF into the BGP routing process:

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

Related Commands

Command	Description
network	Specifies the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.

default-information originate (ipv6 router ospf, router ospf)

To generate a default external route into an OSPFv2 or OSPFv3 routing domain, use the **default-information originate** command in router configuration mode or IPv6 router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]
no default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route whether or not the software has a default route.
metric *value*	(Optional) Specifies the OSPF default metric value, from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) Specifies the external link type associated with the default route advertised into the OSPF routing domain. Valid values are as follows: • **1**—Type 1 external route. • **2**—Type 2 external route.
route-map *map -name*	(Optional) Specifies the name of the route map to apply.

Command Default

The default values are as follows:

- **metric** *value* is 10.
- **metric-type** is 2.

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
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—
Router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for OSPFv3 was added.

Usage Guidelines

Using the **no** form of this command with optional keywords and arguments only removes the optional information from the command. For example, entering the **no default-information originate metric** *3* command removes the **metric** *3* option from the command in the running configuration. To remove the complete command from the running configuration, use the **no** form of the command without any options: **no default-information originate**.

Examples

The following example shows how to use the **default-information originate** command with an optional metric and metric type:

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the OSPFv2 commands in the global router configuration.
ipv6 router ospf	Enters IPv6 router configuration mode.
show running-config ipv6 router	Displays the OSPFv3 commands in the global router configuration.

default-information originate (router rip)

To generate a default route into RIP, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *name*]
no default-information originate [**route-map** *name*]

Syntax Description

route-map *name*	(Optional) Name of the route map to apply. The routing process generates the default route if the route map is satisfied.

Command Default

This command 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
Router rip configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The route map referenced in the **default-information originate** command cannot use an extended access list; it can use only a standard access list.

Examples

The following example shows how to generate a default route into RIP:

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

Related Commands

Command	Description
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

default-language

To set the default language displayed on the Clientless SSL VPN pages, use the **default-language** command in webvpn configuration mode.

default-language*language*

Syntax Description

language	Specifies the name of a previously imported translation table.

Command Default

The default language is en-us (English spoken in the United States).

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
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The ASA provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users. The language parameter must use the format defined in RFC-1766 in order to be in proper compliance.

The default language is displayed to Clientless SSL VPN users when they initially connect to the ASA, before logging in. Thereafter, the language displayed is affected by the tunnel group or group policy settings and any customization that they reference.

Examples

The following example changes the default language to Chinese *with the name >Sales:*

```
ciscoasa(config-webvpn)# default-language zh
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

default-mapping-rule

To configure the default mapping rule in a Mapping Address and Port (MAP) domain, use the **default-mapping-rule** command in MAP domain configuration mode. Use the **no** form of this command to delete the basic mapping rule.

default-mapping-rule *ipv6_prefix / prefix_length*
no default-mapping-rule *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	The IPv6 prefix to be used to embed IPv4 destination addresses per RFC 6052. The prefix length should normally be 64, but allowed values are 32, 40, 48, 56, 64 or 96. Any trailing bits after the embedded IPv4 address are set to 0.

Command Default

No defaults.

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
MAP domain configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The border relay (BR) device uses this rule to translate all IPv4 addresses outside the MAP domain to an IPv6 address that works within the MAP domain. The MAP-T customer edge (CE) devices within the MAP domain install an IPv4 default route using this rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024
```

```
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

default-mcast-group

To specify a default multicast group for all VXLAN VNI interfaces associated with the VTEP source interface, use the **default-mcast-group** command in nve configuration mode. To remove the default group, use the **no** form of this command.

default-mcast-group*mcast_ip*
no default-mcast-group

Syntax Description

mcast_ip	Sets the default multicast group IP address, IPv4 or IPv6.

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
Nve configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.
9.20(1)	This command now supports IPv6.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface (or on the VTEP as a whole with the **default-mcast-address** command).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

If you do not configure the multicast group per VNI interface, then the default group is used. If you configure a group at the VNI interface level, then that group overrides this setting.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and specifies a default multicast group of 236.0.0.100:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.

Command	Description
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

default-metric

To specify the EIGRP metrics for redistributed routes, use the **default-metric** command in router configuration mode. To restore the default values, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*
no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

bandwidth	The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
delay	The route delay in tens of microseconds. Valid values are 1 to any positive number that is a multiple of 39.1 nanoseconds.
loading	The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
mtu	The smallest allowed value for the MTU, expressed in bytes. Valid values are from 1 to 65535.
reliability	The likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.

Command Default

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to the metric of the interface. The metric of redistributed static route with exit interface is the metric of the exit interface. The metric of another EIGRP instance is copied from that instance.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Support for EIGRP Ipv6 routing was added.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP unless you use the **metric** keyword and attributes in the **redistribute** command. Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values. Keeping the same metrics is supported only when you are redistributing from static routes.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

Examples

The following example shows how the redistributed RIP route metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters router configuration mode for that process.
redistribute (EIGRP)	Redistributes routes into the EIGRP routing process.

default user group

For Cloud Web Security, to specify the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA, use the **default user group** command in parameters configuration mode. To remove the default user or group, use the **no** form of this command. You can access the parameters configuration mode by first entering the **policy-map type inspect scansafe** command.

default { [**user** *username* [**group** *groupname*] }
no default [**user** *username* [**group** *groupname*]

Syntax Description

username	Specifies the default username.
groupname	Specifies the default group name.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

If the ASA cannot determine the identity of the user coming into the ASA, then the default user and/or group is included in the HTTP header.

Examples

The following example sets a default name as “Boulder” and a group name as “Cisco”:

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.

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

delay

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

delay*delay-time*
no delay

Syntax Description

delay-time	The delay time in tens of microseconds. Valid values are from 1 to 16777215.

Command Default

The default delay depends upon the interface type. Use the **show interface** command to see the delay value for an interface.

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
8.0(2)	This command was added.
9.1(6)	Support for multiple context mode was added.

Usage Guidelines

The value entered is in tens of microseconds. The delay value displayed in the **show interface** output is in microseconds.

Examples

The following example changes the delay on an interface from the default 1000 to 2000. Truncated **show interface** command output is included before and after the **delay** command to show how the command affects the delay values. The delay value is noted in the second line of the **show interface** output, after the DLY label.

Notice that the command entered to change the delay value to 2000 is **delay 200**, not **delay 2000**. This is because the value entered with the **delay** command is in tens of microseconds, and the **show interface** output displays microseconds.

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output
```

```
removedciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
       IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output removed
```

Related Commands

Command	Description
show interface	Displays interface statistics and settings.

delete

To delete a file from flash memory, use the **delete** command in privileged EXEC mode.

delete [**/noconfirm**] [**/replicate**] [**disk0:| disk1:| flash:**] [*path /*] *filename*

Syntax Description

/noconfirm	(Optional) Does not prompt for confirmation.
/**recursive**	(Optional) Deletes the specified file recursively in all subdirectories.
/replicate	(Optional) Deletes the specified file on the standby unit.
disk0:	(Optional) Specifies the internal flash memory.
disk1:	(Optional) Specifies the external flash memory card.
filename	Specifies the name of the file to delete.
flash:	(Optional) Specifies the internal flash memory. This keyword is the same as **disk0**.
path/	(Optional) Specifies to the path to the file.

Command Default

If you do not specify a directory, the directory is the current working directory 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files. When deleting files, you are prompted with the filename and must confirm the deletion.

Examples

The following example shows how to delete a file named test.cfg in the current working directory:

```
ciscoasa# delete test.cfg
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
rmdir	Removes a file or directory.
show file	Displays the specified file.

deny-message

To change the message delivered to a remote user who logs into WebVPN successfully, but has no VPN privileges, use the **deny-message value** command in group-webvpn configuration mode. To remove the string so that the remote user does not receive a message, use the **no** form of this command.

deny-message value *string*
no deny-message value

Syntax Description

string	Allows up to 491 alphanumeric characters, including special characters, spaces, and punctuation.

Command Default

The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

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-webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command moved from tunnel-group webvpn configuration mode to group-webvpn configuration mode.

Usage Guidelines

Before entering this command, you must enter the **group-policy** *name* **attributes** command in global configuration mode, then the **webvpn** command. (This step assumes you already have created the policy name.)

The **no deny-message none** command removes the attribute from the group-webvpn configuration. The policy inherits the attribute value.

When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The text appears on the remote user's browser upon login, independent of the tunnel policy used for the VPN session.

Examples

The following example shows the first command that creates an internal group policy named group2. The subsequent commands modify the deny message associated with that policy:

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator for
more information."
ciscoasa(config-group-webvpn)
```

Related Commands

Command	Description
clear configure group-policy	Removes all group policy configuration.
group-policy	Creates a group policy.
group-policy attributes	Enters the group-policy attribute configuration mode.
show running-config group-policy	Displays the running group policy configuration for the policy named.
webvpn	Enters group-policy webvpn configuration mode.

deny version

To deny a specific version of SNMP traffic, use the **deny version** command in snmp-map configuration mode. To disable this command, use the **no** form of this command.

deny version *version*
no deny version *version*

Syntax Description

version Specifies the version of SNMP traffic that the ASA drops. The permitted values are **1**, **2**, **2c**, and **3**.

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
Snmp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **deny version** command to restrict SNMP traffic to specific versions of SNMP. Earlier versions of SNMP were less secure, so restricting SNMP traffic to Version 2 may be specified by your security policy. You use the **deny version** command within an SNMP map, which you configure using the **snmp-map** command, which is accessible by entering the **snmp-map** command in global configuration mode. After creating the SNMP map, you enable the map using the **inspect snmp** command, and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface:

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
```

```
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect snmp	Enables SNMP application inspection.
policy-map	Associates a class map with specific security actions.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
service-policy	Applies a policy map to one or more interfaces.

description

To add a description for a named configuration unit (for example, for a context or for an object group, or for a DAP record), use the **description** command in various configuration modes. To remove the description, use the **no** form of this command.

description*text*
no description

Syntax Description

text	Sets the description as a text string of up to 200 characters in length. The description adds helpful notes in your configuration. For dynamic-access-policy-record mode, the maximum length is 80 characters. For event manager applets, the maximum length is 256 characters. If you want to include a question mark (?) in the string, you must type **Ctrl-V** before typing the question mark so you do not inadvertently invoke CLI help.

Command Default

No default behavior or values.

Command Modes

This command is available in various configuration modes.

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Support was added for the dynamic-access-policy-record configuration mode.
9.2(1)	Support for the event manager applet configuration mode was added.

Examples

The following example adds a description to the "Administration" context configuration:

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)
# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)
# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)
# config-url flash://admin.cfg
```

Related Commands

Command	Description
class-map	Identifies traffic to which you apply actions in the **policy-map** command.
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
object-group	Identifies traffic to include in the **access-list** command.

Command	Description
policy-map	Identifies actions to apply to traffic identified by the **class-map** command.