
# default through dhcp-server Commands

# 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.

## Defaults

No default behaviors or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Crl configure configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(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:<br>`default activation key` |

## Defaults

No default behaviors or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

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

## Related Commands

| Command | Description |
|---|---|
| **interface** | Enters interface configuration mode. |

# default (OSPFv3)

To return an OSPFv3 parameter to its default value, use the **default** command in router 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) Spoecifies the OSPFv3 timers. |

## Defaults

No default behaviors or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Router configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 9.0(1) | This command was introduced. |

## Usage Guidelines

Use this command to reset OSPFv3 parameter default values.

## Examples

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

```
hostname(config-router)# default 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 (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.<br>This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are:<br>• daily—Monday through Sunday<br>• weekdays—Monday through Friday<br>• weekend—Saturday and Sunday<br>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." |

## Defaults

No default behavior or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Time-range configuration | • | • | • | • | |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

```
hostname(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 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:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Parameters configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 9.0(1) | We introduced this command. |

## 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”:

```
hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(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. |
| **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. |

# 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. |

## Defaults

No default behavior or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Nac-policy-nac-framework configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |
| 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:

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

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

```
hostname(config-group-policy)# no default-acl
hostname(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 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.

## Defaults

No default behavior or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Crypto ca trustpoint configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# default enrollment
hostname(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-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. |

## Defaults

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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 AnyConnect Secure Mobility 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:

```
hostname(config)# group-policy FirstGroup attributes
hostname(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-group-policy

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. |

## Defaults

The default group name is DfltGrpPolicy.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Tunnel-group general-attributes configuration | • | — | • | — | — |

## Command History

| Version | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 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.

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)# authentication-server-group aaa-server456
```

```
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(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-group-policy (webvpn)

To specify the name of the group policy to use when the WebVPN or 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*

**no default-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. |

## Defaults

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 for WebVPN and 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:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Webvpn configuration | • | — | • | — | — |
| Imap4s configuration | • | — | • | — | — |
| Pop3s configuration | • | — | • | — | — |
| Smtps configuration | • | — | • | — | — |

## Command History

| Version | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 7.1(1) | This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode. |

## Usage Guidelines

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

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 configuration 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 |
| ip-phone-bypass | disabled |
| leap-bypass | disabled |
| nem | disabled |
| **webvpn attributes** | |
| filter | none |
| functions | disabled |
| homepage | none |
| html-content-filter | none |
| port-forward | disabled |
| port-forward-name | none |
| url-list | none |

## Examples

The following example shows how to specify a default group policy called WebVPN7 for WebVPN:

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

# 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). |

## Defaults

1800 seconds (30 minutes).

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Webvpn configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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):

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

**Related Commands**

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

# default-information (EIGRP)

To control the candidate default route information for the EIGRP routing process, use the **default-information** command in router 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. |

## Defaults

Exterior routes are accepted and sent.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |
| 9.0(1) | Multiple context mode is supported. |

## 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:

```
hostname(config)# router eigrp 100
hostname(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 (OSPFv2 and OSPFv3)

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:<br>• **1**—Type 1 external route.<br>• **2**—Type 2 external route. |
| **route-map** *map-name* | (Optional) Specifies the name of the route map to apply. |

## Defaults

The default values are as follows:

- **metric** *value* is 1.
- **metric-type** is 2.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| IPv6 router configuration | • | — | • | — | — |
| Router configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 9.0(1) | Added support for OSPFv3. |

## 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:

```
hostname(config-rtr)# default-information originate always metric 3 metric-type 2
hostname(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 (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. |

## Defaults

This command is disabled by default.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## 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:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(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. |

## Defaults

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:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Webvpn configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |

## 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 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*:

```
hostname(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-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 4294967295. |
| *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. |

## Defaults

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |
| 9.0(1) | Multiple context mode is supported. |

## 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.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 172.16.0.0
hostname(config-router)# redistribute rip
hostname(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. |

# 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. |

## Defaults

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:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |
| 9.0(1) | Multiple context mode is supported. |

## 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.

```
hostname(config)# interface Ethernet0/0
hostname(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 removed

hostname(config-if)# delay 200
hostname(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**] [**/recursive**] [**disk0: | disk1: | flash:**] [*path/*] *filename*

## Syntax Description

| | |
|---|---|
| **/noconfirm** | (Optional) Does not prompt for confirmation. |
| **/recursive** | (Optional) Deletes the specified file recursively in all subdirectories. |
| **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. |

## Defaults

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:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

```
hostname# delete test.cfg
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory to the one specified. |

| Command | Description |
|---|---|
| **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. |

## Defaults

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:

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 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:

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(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."
hostname(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**. |

## Defaults

No default behavior or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Snmp-map configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## 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:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
```

```
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(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.<br>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. |

## Defaults

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 introduced. |
| 8.0(2) | Support was added for the dynamic-access-policy-record configuration mode. |

## Examples

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

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(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. |
| **gtp-map** | Controls parameters for the GTP inspection engine. |
| **interface** | Configures an interface and enters interface configuration mode. |
| **object-group** | Identifies traffic to include in the **access-list** command. |
| **policy-map** | Identifies actions to apply to traffic identified by the **class-map** command. |

# dhcp client route distance

To configure an administrative distance for routes learned through DHCP, use the **dhcp client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

**dhcp client route distance** *distance*

**no dhcp client route distance** *distance*

## Syntax Description

| | |
|---|---|
| *distance* | The administrative distance to apply to routes learned through DHCP. Valid values are from 1 to 255. |

## Defaults

Routes learned through DHCP are given an administrative distance of 1 by default.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Usage Guidelines

The **dhcp client route distance** command is checked only when a route is learned from DHCP. If the **dhcp client route distance** command is entered after a route is learned from DHCP, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

## Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
```

```
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

## Related Commands

| Command | Description |
|---|---|
| **dhcp client route track** | Associates routes learned through DHCP with a tracking entry object. |
| **ip address dhcp** | Configures the specified interface with an IP address obtained through DHCP. |
| **sla monitor** | Defines an SLA monitoring operation. |
| **track rtr** | Creates a tracking entry to poll the SLA. |

# dhcp client route track

To configure the DHCP client to associate added routes with a specified tracked object number, use the **dhcp client route track** command in interface configuration mode. To disable DHCP client route tracking, use the **no** form of this command.

**dhcp client route track** *number*

**no dhcp client route track**

## Syntax Description

| | |
|---|---|
| *number* | The tracking entry object ID. Valid values are from 1 to 500. |

## Defaults

No default behaviors or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Usage Guidelines

The **dhcp client route track** command is checked only when a route is learned from DHCP. If the **dhcp client route track** command is entered after a route is learned from DHCP, the existing learned routes are not associated with a tracking object. You must put the following two commands in the correct order. Make sure that you always enter the **dhcp client route track** command first, followed by the **ip address dhcp setroute** command, If you have already entered the **ip address dhcp setroute** command, then remove it and reenter it in the order previously described. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option in the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

## Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
```

```
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

## Related Commands

| Command | Description |
|---|---|
| **dhcp client route distance** | Assigns an administrative distance to routes learned through DHCP. |
| **ip address dhcp** | Configures the specified interface with an IP address obtained through DHCP. |
| **sla monitor** | Defines an SLA monitoring operation. |
| **track rtr** | Creates a tracking entry to poll the SLA. |

# dhcp-client broadcast-flag

To allow the ASA to set the broadcast flag in the DHCP client packet, use the **dhcp-client broadcast-flag** command in global configuration mode. To disallow the broadcast flag, use the **no** form of this command.

**dhcp-client broadcast-flag**

**no dhcp-client broadcast-flag**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, the broadcast flag is disabled.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |

## Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

## Examples

The following example enables the broadcast flag:

```
hostname(config)# dhcp-client broadcast-flag
```

## Related Commands

| Command | Description |
|---|---|
| **ip address dhcp** | Enables the DHCP client for an interface. |
| **interface** | Enters interface configuration mode so you can set the IP address. |

| | |
|---|---|
| **dhcp-client client-id** | Sets DHCP request packet option 61 to include the interface MAC address. |
| **dhcp-client update dns** | Enables DNS updates for the DHCP client. |

# dhcp-client client-id

To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally generated string, use the **dhcp-client client-id** command in global configuration mode. To disallow the MAC address, use the **no** form of this command.

**dhcp-client client-id interface** *interface_name*

**no dhcp-client client-id interface** *interface_name*

## Syntax Description

| | |
|---|---|
| **interface** *interface_name* | Specifies the interface on which you want to enable the MAC address for option 61. |

## Defaults

By default, an internally-generated ASCII string is used for option 61.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |

## Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use the **dhcp-client client-id** command to include the interface MAC address for option 61.

## Examples

The following example enables the MAC address for option 61 for the outside interface:

```
hostname(config)# dhcp-client client-id interface outside
```

## Related Commands

| Command | Description |
|---|---|
| **ip address dhcp** | Enables the DHCP client for an interface. |
| **interface** | Enters interface configuration mode so you can set the IP address. |

| | |
|---|---|
| **dhcp-client broadcast-flag** | Sets the broadcast flag in the DHCP client packet. |
| **dhcp-client update dns** | Enables DNS updates for the DHCP client. |

# dhcp-client update dns

To configure the update parameters that the DHCP client passes to the DHCP server, use the **dhcp-client update dns** command in global configuration mode. To remove the parameters that the DHCP client passes to the DHCP server, use the **no** form of this command.

**dhcp-client update dns** [**server** {**both** | **none**}]

**no dhcp-client update dns** [**server** {**both** | **none**}]

## Syntax Description

| | |
|---|---|
| **both** | The client requests that the DHCP server update both the DNS A and PTR resource records. |
| **none** | The client requests that the DHCP server perform no DDNS updates. |
| **server** | Specifies the DHCP server to receive the client requests. |

## Defaults

By default, the ASA requests that the DHCP server perform PTR RR updates only. The client does not send the FQDN option to the server.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Usage Guidelines

This command can also be entered in interface configuration mode, but it is not hyphenated. See the **dhcp client update dns** command. When entered in interface mode, the **dhcp client update dns** command overrides settings configured by this command in global configuration mode.

## Examples

The following example configures the client to request that the DHCP server update neither the A and the PTR RRs:

```
hostname(config)# dhcp-client update dns server none
```

The following example configures the client to request that the server update both the A and PTR RRs:

```
hostname(config)# dhcp-client update dns server both
```

## Related Commands

| Command | Description |
|---|---|
| **ddns** | Specifies a DDNS update method type for a created DDNS method. |
| **ddns update** | Associates a DDNS update method with a ASA interface or a DDNS update hostname. |
| **ddns update method** | Creates a method for dynamically updating DNS resource records. |
| **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. |

# dhcp-network-scope

To specify the range of IP addresses the ASA DHCP server should use to assign addresses to users of this group policy, use the **dhcp-network-scope** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

**dhcp-network-scope** {*ip_address*} | **none**

**no dhcp-network-scope**

## Syntax Description

| | |
|---|---|
| *ip_address* | Specifies the IP subnetwork the DHCP server should use to assign IP addresses to users of this group policy. |
| **none** | Sets the DHCP subnetwork to a null value, thereby allowing no IP addresses. Prevents inheriting a value from a default or specified group policy. |

## Defaults

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

This command allows inheritance of a value from another group policy. To prevent inheriting a value, use the **dhcp-network-scope none** command.

## Examples

The following example shows how to set an IP subnetwork of 10.10.85.1 for the group policy named First Group:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.1
```

# dhcp-server

To configure support for DHCP servers that assign IP addresses to clients as a VPN tunnel is established, use the **dhcp-server** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

**dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

## Syntax Description

| | |
|---|---|
| **ip1** | Address of a DHCP server |
| **ip2-ip10** | (Optional) Addresses of additional DHCP servers. Up to ten may be specified in the same command or spread over multiple commands. |
| **link-selection** | (Optional) Specifies that the ASA should send DHCP suboption 5, the Link Selection Suboption for the Relay Information Option 82, defined by RFC 3527. This should only be used with servers that support this RFC. |
| **subnet-selection** | (Optional) Specifies that the ASA should send DHCP Option 118, the IPv4 Subnet Selection Option, defined by RFC 3011. This should only be used with servers that support this RFC. |

## Defaults

No default behavior or values.

## Command Modes

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

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Tunnel-group general attributes configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 8.0(5) | Added the **link-selection** and **subnet-selection** keywords. |

## Usage Guidelines

You can apply this attribute to remote access tunnel group types only.

## Examples

The following command, entered in config-general configuration mode, adds three DHCP servers (dhcp1, dhcp2, and dhcp3) to the IPsec remote access tunnel group “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type remote-access
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
```

```
hostname(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-tunnel-general)
```

## Related Commands

| Command | Description |
|---|---|
| **clear-configure tunnel-group** | Clears all configured tunnel groups. |
| **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. |