



# Certificate Policy Configuration Mode Commands

Configure the context level name to be used for the IKEv2 Security Association Certificate Policy for the current context.

## Command Modes

Exec > Global Configuration > Context Configuration > Certificate Policy Configuration

**configure** > **context** *context\_name* **Certificate Policy Configuration** *service\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cert-policy) #
```

- [do show, on page 1](#)
- [end, on page 2](#)
- [exit, on page 2](#)
- [id, on page 2](#)

## do show

Executes all **show** commands while in Configuration mode.

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**do show**

### Usage Guidelines

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



### Caution

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

## end

Exits the current configuration mode and returns to the Exec mode.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

Exits the current mode and returns to the parent configuration mode.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## id

Configures ID for cert-entry.

<b>Product</b>	SecGW
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context <b>configure &gt; context</b> <i>context_name</i> <b>ikev2-ikesa</b> <i>ikev2_sec_para</i> Entering the above command sequence results in the following prompt: [local] <i>host_name</i> (config-cert-policy)#
<b>Syntax Description</b>	<b>epdg-s2b-gtpv2 send</b> <i>value</i> <b>match-criteria</b> { <b>common-name</b> <i>value</i> <i>value</i>   <b>domain-name</b> <i>value</i> <i>value</i> }  <b>id</b> <i>value</i> <i>value</i> : is an integer between 1 and 64.

**match-criteria**

Configures the match criteria to be configured and used for peer using cert as authorization for given Crypto Template.

**common-name valuevalue**

Configures the entry with match criteria as common-name to be matched with CN in received Certificate.

*value*: is a string of size 1 through 64.

**domain-name valuevalue**

Configure the entry with match criteria as domain name to be matched with domain in received Certificate.

*value*: is a string of size 1 through 64.

---

**Usage Guidelines**

Use this command to Enable/Disable the inclusion of the "UE Local IP Address" and "UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

**Example**

Use the following command to configure ID for certificate entry as 4 with match criteria as domain name dom1.

```
id 4 match-criteria domain-name dom1
```

id