

# EAP Authentication Configuration Mode Commands

**Command Modes**

The EAP Authentication Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication methods for the crypto template.

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

**configure > context** *context_name* **> crypto template** *template_name* **ikev2-dynamic > authentication eap-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Important** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).


- eap-aka, on page 1
- eap-gtc, on page 2
- eap-md5, on page 3
- end, on page 4
- exit, on page 4


# eap-aka

Configures shared key values for the Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) authentication method used by subscribers using this crypto template.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

**configure > context** *context_name* **> crypto template** *template_name* **ikev2-dynamic > authentication eap-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Syntax Description**

```
eap-aka { encrypted key hex | key hex }
```

**encrypted key *hex***

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string or a hexadecimal number beginning with "0x".

**key *hex***

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string or a hexadecimal number beginning with "0x".

**Usage Guidelines**

Use this command to set shared key parameters for subscribers using the EAP-AKA authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-AKA method:

```
eap-aka key aa11223344556677
```

# eap-gtc

Configures shared key values for the EAP-GTC authentication method used by subscribers using this crypto template.

**Product**

ASN-GW

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

**configure > context** *context_name* **> crypto template** *template_name* **ikev2-dynamic > authentication eap-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Syntax Description**

```
eap-gtc { encrypted key value | key value }
```

**encrypted key *value***

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

**key *value***

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

**Usage Guidelines**

Use this command to set shared key parameters for subscribers using the EAP-GTC authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-GTC method:

```
eap-gtc key aa11223344556677
```

# eap-md5

Configures shared key values for the EAP-MD5 authentication method used by subscribers using this crypto template.

**Product**

ASN-GW

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

**configure > context** *context_name* **> crypto template** *template_name* **ikev2-dynamic > authentication eap-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Syntax Description**

**eap-md5 { encrypted key** *value* **| key** *value* **}**

**encrypted key *value***

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

**key *value***

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

**Usage Guidelines**

Use this command to set shared key parameters for subscribers using the EAP-MD5 authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-MD5 method:

```
eap-md5 key aa11223344556677
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

**Usage Guidelines** Use this command to return to the parent configuration mode.