PKI Certificate Authority Configuration Mode Commands

To configure public key infrastructure (PKI) encryption certificate authorities on a WAAS device, use the **crypto pki ca** global configuration command. To delete a PKI encryption certificate authority, use the **no** form of the command.

crypto pki ca *certificate_authority_name*

no crypto pki ca *certificate_authority_name*

Syntax Description

certificate_authority_name	Name of the certificate authority (CA). The CA name may contain up to 64 characters.

Defaults

No default behavior or values.

Command Modes

global configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Use the command to add and configure a certificate authority. This command initiates the certificate authority configuration mode, indicated by the **(config-ca)** prompt.

Within certificate authority configuration mode, you can use the various commands (**ca-certificate**, **description**, **revocation check**, and so on) to define an encryption certificate authority. To return to global configuration mode, enter **exit** at the certificate authority configuration mode prompt.

Examples

The following example shows how to create or edit a certificate authority named mycertauth. If the certificate authority is already established on the WAAS device, the **crypto pki ca** command edits it. If the certificate authority does not exist, the **crypto pki ca** command creates it.

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# description This-is-my-CA-description
WAE(config-ca)# exit
WAE(config)#
```

Related Commands

(config-ca) ca-certificate

(config-ca) ca-certificate

To set the certification authority file to be used by the WAAS device, use the **ca-certificate** certification authority configuration command.

ca-certificate *filename.ca*

Syntax Description		
	filename.ca	Filename of the certificate authority. The filename must end in .ca and be no longer than 32 characters.

Defaults

No default behavior or values.

Command Modes

certification authority configuration

Device Modes

application-accelerator

central-manager

Usage Guidelines

Before you can assign a certification authority file using the **ca-certificate** command, the certification authority file must be imported using the **crypto import ca-certificate** EXEC command. See the crypto import command.

Examples

The following example shows how to specify the certification authority file to use:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# ca-certificate mycafile.ca
```

Related Commands

(config-ca) description

(config-ca) revocation-check

(config-ca) description

To enter a description for the certification authority to be used by the WAAS device, use the **description** command.

description *description-text*

Syntax Description		
	description-text	Test to briefly describe the certification authority being used. The description text must not exceed 128 characters.

Defaults

No default behavior or values.

Command Modes

certification authority configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to define the descriptive text for the certification authority:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# description This is my CA description
```

Related Commands

(config-ca) ca-certificate

(config-ca) revocation-check

(config-ca) revocation-check

To configure the certification authority revocation checking method, use the **revocation-check** command.

revocation-check {**none** | **ocsp-cert-url** | **ocsp-url**} [**none** | **ocsp-cert-url** | **ocsp-url**]

Syntax Description

none	No revocation checking is used.
ocsp-cert-url	Enables Online Certificate Status Protocol (OCSP) revocation status checking using the CA server URL defined in the CA certificate.
ocsp-url	Enables OCSP revocation status checking using the URL defined for the global OCSP settings.

Defaults

No default behavior or values.

Command Modes

certification authority configuration

Device Modes

application-accelerator

central-manager

Examples

The following example shows how to configure certification authority revocation checking to use the URL defined in the global OCSP settings:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# revocation-check ocsp-url
```

The following example shows how to configure revocation checking to use the URL defined in the global OCSP settings as the first method, and to use no checking as the second method:

```
WAE(config)# crypto pki ca mycertauth
WAE(config-ca)# revocation-check ocsp-url none
```

Related Commands

(config-ca) ca-certificate

(config-ca) description