

Configuration Statements for Configuring Digital Certificates for an ES PIC

To define the digital certificate configuration for an encryption service interface, include the following statements at the [edit security certificates] and [edit security ike] hierarchy levels:

```
[edit security]
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-filename {
    certificate-key-string;
    load-key-file key-file-name;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
ike {
  policy ike-peer-address {
    description policy;
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
  }
}
```

The statements for configuring digital certificates differ for the AS and MultiServices PICs and the ES PIC.

For information about how to configure the **description** and **mode** statements, see [Configuring an IKE Policy for Preshared Keys](#) and [Configuring an IKE Policy for Preshared Keys](#). For information about how to configure the IKE proposal, see [Configuring an IKE Policy for Preshared Keys](#).



NOTE: For digital certificates, the JUNOS Software supports only VeriSign CAs for the ES PIC.

Related Topics ■ Digital Certificates Overview

Published: 2010-04-26