

Chapter 33

Summary of Security Services Configuration Statements

The following sections explain each of the security services configuration statements. The statements are organized alphabetically.

authentication

Syntax	authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); }
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Description	Configure IP Security (IPSec) authentication parameters for manual security association (SA).
Options	algorithm—Hash algorithm that authenticates packet data. It can be one of the following: hmac-md5-96—Produces a 128-bit digest. hmac-sha1-96—Produces a 160-bit digest. key—Type of authentication key. It can be one of the following: ascii-text <i>key</i> —ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters. hexadecimal <i>key</i> —Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.
Usage Guidelines	See “Configuring the Authentication Algorithm and Key” on page 631.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm

See the following sections:

authentication-algorithm (IKE) on page 666

authentication-algorithm (IPSec) on page 666

authentication-algorithm (IKE)

Syntax	authentication-algorithm (md5 sha1);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the Internet Key Exchange (IKE) authentication algorithm.
Options	authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms: <ul style="list-style-type: none"> md5—Produces a 128-bit digest. sha1—Produces a 160-bit digest.
Usage Guidelines	See “Configuring the Authentication Algorithm for an IKE Proposal” on page 634.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-algorithm (IPSec)

Syntax	authentication-algorithm (hmac-md5-96 hmac-sha1-96);
Hierarchy Level	[edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure the IPSec authentication algorithm.
Options	authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms: <ul style="list-style-type: none"> hmac-md5-96—Produces a 128-bit digest. hmac-sha1-96—Produces a 160-bit digest.
Usage Guidelines	See “Configuring the Authentication Algorithm for an IPSec Proposal” on page 641.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

authentication-method

Syntax	authentication-method (dsa-signatures pre-shared-keys rsa-signatures);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the IKE authentication method.
Options	<p>dsa-signatures—Digital Signature Algorithm (DSA)</p> <p>rsa-signatures—A public key algorithm, which supports encryption and digital signatures</p> <p>pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange</p>
Usage Guidelines	See “Configuring the Authentication Method for an IKE Proposal” on page 635.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

auxiliary-spi

Syntax	auxiliary-spi <i>auxiliary-spi-value</i> ;
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Description	Configure the auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
Options	<p><i>auxiliary-spi-value</i>—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).</p> <p>Range: 256 through 16,639</p>
Usage Guidelines	See “Configuring the Auxiliary Security Parameter Index” on page 630. For information about SPI, see “Configuring the Security Parameter Index” on page 630 and spi on page 690.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

ca-name

Syntax	<code>ca-name <i>ca-identity</i>;</code>
Hierarchy Level	[edit security certificates certification-authority]
Description	Specify the certificate authority (CA) identity to use in the certificate request.
Usage Guidelines	See “Specifying the Certificate Authority Name” on page 649.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

cache-size

Syntax	<code>cache-size <i>bytes</i>;</code>
Hierarchy Level	[edit security certificates]
Description	Configure the cache size for digital certificates.
Options	<i>bytes</i> —Cache size for digital certificates. Range: 64 through 4,294,967,295 Default: 2 megabytes (MB)



NOTE: We recommend that you limit your cache size to 4 MB.

Usage Guidelines	See “Configuring the Cache Size” on page 651.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration

cache-timeout-negative

Syntax	cache-timeout-negative <i>seconds</i> ;
Hierarchy Level	[edit security certificates]
Description	Configure a negative cache for digital certificates.
Options	<i>seconds</i> —Negative time to cache digital certificates, in seconds. Range: 10 through 4,294,967,295 Default: 20



CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.

Usage Guidelines	See “Configuring the Negative Cache” on page 651.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration

certificates

Syntax	<pre> certificates { cache-size <i>bytes</i>; cache-timeout-negative <i>seconds</i>; certification-authority <i>ca-profile-name</i> { ca-name <i>ca-identity</i>; crl <i>file-name</i>; encoding (binary pem); enrollment-url <i>url-name</i>; file <i>certificate-filename</i>; ldap-url <i>url-name</i>; } enrollment-retry <i>attempts</i>; local <i>certificate-filename</i> { <i>certificate-key-string</i>; load-key-file <i>key-filename</i>; } maximum-certificates <i>number</i>; path-length <i>certificate-path-length</i>; } </pre>
Hierarchy Level	[edit security]
Description	Configure the digital certificates for IPsec.
Usage Guidelines	See “Configuring Digital Certificates” on page 645.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

certification-authority

Syntax certification-authority *ca-profile-name* {
 ca-name *ca-identity*;
 crl *file-name*;
 encoding (binary | pem);
 enrollment-url *url-name*;
 file *certificate-filename*;
 ldap-url *url-name*;
 }

Hierarchy Level [edit security certificates]

Description Configure a certificate authority profile name. The remaining statements are explained separately.

Usage Guidelines See “Configuring the Certificate Authority Properties” on page 649.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration

crl

Syntax crl *file-name*;

Hierarchy Level [edit security certificates]

Description Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options *file-name*—Specifies the file from which to read the CRL.

Usage Guidelines See “Configuring the Certificate Authority Properties” on page 649.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration

description

Syntax	<code>description <i>description</i>;</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec policy <i>ipsec-policy-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>], [edit security ipsec security-association <i>sa-name</i>]
Description	Specify a text description for an IKE proposal or policy, or an IPsec proposal, policy, or SA.
Usage Guidelines	See “Configuring the Description for an IKE Proposal” on page 635, “Configuring the Description for an IKE Policy” on page 638,
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

dh-group

Syntax	<code>dh-group (group1 group2);</code>
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Description	Configure the IKE Diffie-Hellman group.
Options	dh-group—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. It can be one of the following: group1—768-bit. group2—1024-bit.
Usage Guidelines	See “Configuring the Diffie-Hellman Group for an IKE Proposal” on page 635.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

direction

Syntax direction (inbound | outbound | bi-directional) {
 authentication {
 algorithm (hmac-md5-96 | hmac-sha1-96);
 key (ascii-text *key* | hexadecimal *key*);
 }
 auxiliary-spi *auxiliary-spi-value*;
 encryption {
 algorithm (des-cbc | 3des-cbc);
 key (ascii-text *key* | hexadecimal *key*);
 }
 protocol (ah | esp | bundle);
 spi *spi-value*;
 }

Hierarchy Level [edit security ipsec security-association *sa-name* manual]

Description Define the direction of IPSec processing.

Options inbound—Inbound SA.
 outbound—Outbound SA.
 bidirectional—Bidirectional SA.

Usage Guidelines See “Configuring the Processing Direction” on page 628.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.


dynamic

Syntax	dynamic { ipsec-policy <i>ipsec-policy-name</i> ; replay-window-size (32 64); }
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define a dynamic IPsec SA.
Options	ipsec-policy <i>ipsec-policy-name</i> —Name of the IPsec policy. replay-window-size—(Optional) Antireplay window size. It can be one of the following values: 32—32-packet window size. 64—64-packet window size.
Usage Guidelines	See “Configuring Dynamic Security Associations” on page 633 and “Configuring the ES PIC” on page 656.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

encoding

Syntax	encoding (binary pem);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security certificates certification-authority <i>ca-profile-name</i>]
Description	Specify the file format used for the local-certificate and local-key-pair statements.
Options	binary—Binary file format. pem—Privacy-enhanced mail (PEM), an ASCII base64 encoded format. Default: binary
Usage Guidelines	See “Configuring the Type of Encoding Your CA Supports” on page 650 and “Configuring the Type of Encoding Your CA Supports” on page 653.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

encryption

Syntax	<pre> encryption { algorithm (des-cbc 3des-cbc); key (ascii-text key hexadecimal key); } </pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bidirectional)]
Description	Configure an encryption algorithm and key for manual SA.
Options	<p>algorithm—Type of encryption algorithm. It can be one of the following:</p> <ul style="list-style-type: none"> des-cbc—Has a block size of 8 bytes (64 bits); its key size is 48 bits long. 3des-cbc—Has block size of 8 bytes (64 bits); its key size is 192 bits long.
	<p>NOTE: For 3des-cbc, we recommend that the first 8 bytes are not the same as the second 8 bytes, and the second 8 bytes are the same as the third 8 bytes.</p>
	<p>key—Type of encryption key. It can be one of the following:</p> <ul style="list-style-type: none"> ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters. hexadecimal—Hexadecimal key. For the des-cbc option, the key contains 16 hexadecimal characters; for the 3des-cbc option, the key contains 48 hexadecimal characters.
Usage Guidelines	See “Configuring the Encryption Algorithm and Key” on page 632.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

encryption-algorithm

Syntax	encryption-algorithm (3des-cbc des-cbc);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Description	Configure an IKE or IPSec encryption algorithm.
Options	3des-cbc—Encryption algorithm with key size of 24 bytes; its key size is 192 bits long. des-cbc—Encryption algorithm with key size of 8 bytes; its key size is 48 bits long.
Usage Guidelines	See “Configuring the Encryption Algorithm for an IKE Proposal” on page 636 and “Configuring the Encryption Algorithm for an IPSec Proposal” on page 641.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

enrollment-retry

Syntax	enrollment-retry <i>attempts</i> ;
Hierarchy Level	[edit security certificates]
Description	Specify how many times a router will resend a digital certificate request.
Options	<i>number</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Usage Guidelines	See “Configuring the Number of Enrollment Retries” on page 652
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

enrollment-url

Syntax	enrollment-url <i>url-name</i> ;
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Options	<i>url-name</i> —Certificate authority URL.
Description	Specify where your router should send Simple Certificate Enrollment Protocols-based (SCEP-based) certificate enrollment requests (certificate authority URL).
Usage Guidelines	See “Specifying an Enrollment URL” on page 650.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

file

Syntax	file <i>certificate-filename</i> ;
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Description	Specify the file from which to read the digital certificate.
Options	<i>certificate-filename</i> —File from which to read the digital certificate.
Usage Guidelines	See “Specifying a File to Read the Digital Certificate” on page 650.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

identity

Identity	identity <i>identity-name</i> ;
Hierarchy Level	[edit security ike]
Description	Define the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).
Usage Guidelines	See “Configuring the Identity to Define the Remote Certificate Name” on page 653.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

ike

```

Syntax  ike {
            policy ike-peer-address {
                description policy-description;
                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 ];
            }
            proposal ike-proposal-name {
                authentication-algorithm (md5 | sha1);
                authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
                dh-group (group1 | group2);
                encryption-algorithm (3des-cbc | des-cbc);
                lifetime-seconds seconds;
            }
        }

```

Hierarchy Level [edit security]

Description Configure IKE.

The statements are explained separately.

Usage Guidelines See “Configuring an IKE Proposal (Dynamic SAs Only)” on page 634 and “Configuring an IKE Policy for Preshared Keys” on page 637.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

ipsec

```

Syntax ipsec {
    policy ipsec-policy-name {
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm (3des-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    security-association name {
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bi-directional) {
                authentication {
                    algorithm (hmac-md5-96 | hmac-sha1-96);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi-value;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
                protocol (ah | esp | bundle);
                spi spi-value;
            }
        }
        mode (tunnel | transport);
    }
    traceoptions {
        file <files number> < size size>;
        flag all;
        flag database;
        flag general;
        flag ike;
        flag parse;
        flag policy-manager;
        flag routing-socket;
        flag timer;
    }
}

```

Hierarchy Level [edit security]

Description Configure IPSec.

The statements are explained separately.

Usage Guidelines See “Configuring Security Associations” on page 625.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

ldap-url

Syntax ldap-url *url-name*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Description (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

Options *url*—Name of the LDAP URL.

Usage Guidelines See “Specifying an LDAP URL” on page 651.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

lifetime-seconds

Syntax lifetime-seconds *seconds*;

Hierarchy Level [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]

Description (Optional) Configure the lifetime of IKE or IPsec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.

Options *seconds*—Lifetime, in seconds.
Range: 180 through 86,400

Usage Guidelines See “Configuring the Lifetime for an IKE SA” on page 636 and “Configuring the Lifetime for an IPsec SA” on page 641.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

local

Syntax local *certificate-filename* {
 certificate-key-string;
 load-key-file *key-filename*;
 }

Hierarchy Level [edit security certificates]

Description Import a Secure Sockets Layer (SSL) certificate into the router.



NOTE: Configuring xnm-ssl service does not apply to IPSec.

Options *certificate-filename*—SSL certificate name.

Usage Guidelines See “Using JUNOScript SSL Service” on page 663.

local-certificate

Syntax local-certificate *certificate-filename*;

Hierarchy Level [edit security ike policy *ike-peer-address*]

Description Configure the certificate filename from which to read the local certificate.

Options *certificate-filename*—File from which to read the local certificate.

Usage Guidelines See “Specifying the Certificate Filename” on page 654.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

local-key-pair

Syntax local-key-pair *private-public-key-file*;

Hierarchy Level [edit security ike policy *ike-peer-address*]

Description Specify private and public keys.

Options *private-public-key-file*—Specifies the file from which to read the private and public key pair.

Usage Guidelines See “Specifying the Private and Public Key File” on page 654.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

manual

Syntax	<pre> manual { direction (inbound outbound bi-directional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text key hexadecimal key); } auxiliary-spi auxiliary-spi-value; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text key hexadecimal key); } protocol (ah esp bundle); spi spi-value; } } </pre>
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	<p>Define a manual IPSec SA.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring Manual Security Associations” on page 628.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

maximum-certificates

Syntax	maximum-certificates <i>number</i> ;
Hierarchy Level	[edit security certificates]
Description	Configure the maximum number of peer digital certificates to be cached.
Options	<p><i>number</i>—Maximum number of peer digital certificates to be cached.</p> <p>Range: 64 through 4,294,967,295 peer certificates</p> <p>Default: 1024 peer certificates</p>
Usage Guidelines	See “Configuring the Maximum Number of Peer Certificates” on page 652.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

mode

See the following sections:

mode (IKE) on page 682

mode (IPSec) on page 682

mode (IKE)

Syntax	mode (aggressive main);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define the IKE policy mode.
Options	mode—Type of IKE policy. aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection. main—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection. Default: main
Usage Guidelines	See “Configuring the Mode for an IKE Policy” on page 638.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

mode (IPSec)

Syntax	mode (transport tunnel);
Hierarchy Level	[edit security ipsec security-association <i>name</i>]
Description	Define the mode for the IPSec security association.
Options	transport— Protects traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. Virtual Private Network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. tunnel—Protects traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers. Default: tunnel



NOTE: Tunnel mode requires the ES Physical Interface Card (PIC).

The JUNOS software supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the JUNOS software does not support authentication header (AH) and ESP header bundles.

In transport mode, the JUNOS software supports only Border Gateway Protocol (BGP).

Usage Guidelines See “Configuring IPsec Mode” on page 626.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

path-length

Syntax path-length *certificate-path-length*;

Hierarchy Level [edit security certificates]

Description Configure the digital certificate path length.

Options *certificate-path-length*—Digital certificate path length.
Range: 2 through 15 certificates
Default: 15 certificates

Usage Guidelines See “Configuring the Path Length for the Certificate Hierarchy” on page 652.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

perfect-forward-secrecy

Syntax	<pre>perfect-forward-secrecy { keys (group1 group2); }</pre>
Hierarchy Level	[edit security ipsec policy <i>ipsec-policy-name</i>]
Description	(Optional) Define the Perfect Forward Secrecy (PFS) protocol. Creates single use keys.
Options	<p>keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.</p> <p>The key can be one of the following:</p> <ul style="list-style-type: none">group1—768-bit.group2—1024-bit.
Usage Guidelines	See “Configuring Perfect Forward Secrecy” on page 644.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

policy

See the following sections:

policy (IKE) on page 685

policy (IPSec) on page 686

policy (IKE)

Syntax `policy ike-peer-address {
 description policy-description;
 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];
}`

Hierarchy Level [edit security ike]

Description Define an IKE policy.

Options *ike-peer-address*—A tunnel address configured at the [edit interfaces es] hierarchy level.

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IKE Policy for Preshared Keys” on page 637 and “Configuring an IKE Policy for Digital Certificates” on page 653.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

policy (IPSec)

Syntax	<pre> policy ipsec-policy-name { perfect-forward-secrecy { keys (group1 group2); } proposals [proposal-names]; } </pre>
Hierarchy Level	[edit security ipsec]
Description	Define an IPSec policy.
Options	<p><i>ipsec-policy-name</i>—Specify an IPSec policy name.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring the IPSec Policy” on page 643.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

pre-shared-key

Syntax	pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Description	Define a preshared key for an IKE policy.
Options	<p>pre-shared-key—Type of preshared key.</p> <p>The key can be one of the following:</p> <p> ascii-text—ASCII text key.</p> <p> hexadecimal—Hexadecimal key.</p>
Usage Guidelines	See “Configuring the Preshared Key for an IKE Policy” on page 638.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

proposal

See the following sections:

proposal (IKE) on page 687

proposal (IPSec) on page 687

proposal (IKE)

Syntax `proposal ike-proposal-name {
 authentication-algorithm (md5 | sha1);
 authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
 description description;
 dh-group (group1 | group2);
 encryption-algorithm (3des-cbc | des-cbc);
 lifetime-seconds seconds;
 }`

Hierarchy Level [edit security ike]

Description Define an IKE proposal for a dynamic SA.

Options *ike-proposal-name*—Specifies a IKE proposal name.

The remaining statements are explained separately.

Usage Guidelines See “Configuring an IKE Proposal (Dynamic SAs Only)” on page 634.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

proposal (IPSec)

Syntax `proposal ipsec-proposal-name {
 authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
 encryption-algorithm (3des-cbc | des-cbc);
 lifetime-seconds seconds;
 protocol (ah | esp | bundle);
 }`

Hierarchy Level [edit security ipsec]

Description Define an IPSec proposal for a dynamic SA.

Options *ipsec-proposal-name*—Specifies an IPSec proposal name.

The statements are explained separately.

Usage Guidelines See “Configuring an IPSec Proposal” on page 640.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

proposals

Syntax	<code>proposals [<i>proposal-names</i>];</code>
Hierarchy Level	<code>[edit security ike policy <i>ike-peer-address</i>],</code> <code>[edit security ipsec policy <i>ipsec-policy-name</i>]</code>
Description	Associate one or more proposals with an IKE or IPSec policy.
Options	<i>proposal-names</i> —Name of one or more proposals.
Usage Guidelines	See “Associating Proposals with an IKE Policy” on page 638 and “Configuring the IPSec Policy” on page 643.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

protocol


Syntax	<code>protocol (ah esp bundle);</code>
Hierarchy Level	<code>[edit security ipsec proposal <i>ipsec-proposal-name</i>],</code> <code>[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bidirectional)]</code>
Description	Define the IPSec protocol for a manual or dynamic SA.
Options	ah—Authentication Header protocol bundle—AH and ESP protocols esp—ESP protocol (the tunnel statement must be included at the <code>[edit security ipsec security-association <i>sa-name</i> mode]</code> hierarchy level)
Usage Guidelines	See “Configuring the Protocol for a Manual SA” on page 629 and “Configuring the Protocol for a Dynamic IPSec SA” on page 643.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

security-association

Syntax	<pre> security-association <i>sa-name</i> { dynamic { ipsec-policy <i>policy-name</i>; replay-window-size (32 64); } manual { direction (inbound outbound bi-directional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } auxiliary-spi <i>auxiliary-spi-value</i>; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } protocol (ah esp bundle); spi <i>spi-value</i>; } mode (tunnel transport); } } </pre>
Hierarchy Level	[edit security ipsec]
Options	<p><i>name</i>—Name of the security association.</p> <p>The remaining statements are explained separately.</p>
Description	Configure an IPSec security association.
Usage Guidelines	See “Configuring Security Associations” on page 625.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

spi

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Description	Configure SPI for an SA.
Options	<i>spi-value</i> —An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet). Range: 256 through 16,639

 **NOTE:** Use the auxiliary SPI when you configure the protocol statement to use the bundle option.

Usage Guidelines	See “Configuring the Security Parameter Index” on page 630.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

traceoptions

Syntax	<pre> traceoptions { file filename <files number> <size size>; flag all; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; } </pre>
Hierarchy Level	[edit security]
Description	Configure security tracing options. To specify more than one tracing option, include multiple flag statements. The output of the security tracing options is placed in one file: /var/log/kmd.
Options	<p><i>files number</i>—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option. Range: 2 through 1000 files Default: 10 files</p>

size size—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, *kmd*) reaches this size, it is renamed, *kmd.0*, then *kmd.1* and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple *flag* statements.

all—Trace all security events.

database—Trace database events.

general—Trace general events.

ike—Trace IKE module processing.

parse—Trace configuration processing.

policy-manager—Trace policy manager processing.

routing-socket—Trace routing socket messages.

timer—Trace internal timer events.

Usage Guidelines See “Configuring Trace Options” on page 656.

Required Privilege Level *admin*—To view the configuration.
admin-control—To add this statement to the configuration.

