



IP Security Options Commands

This chapter describes IP Security Options (IPSO) commands. IPSO is generally used to comply with the U.S. Government's Department of Defense security policy.

Refer to the *Command Reference Master Index* or search online to find complete descriptions of other commands used when configuring IPSO.

For IPSO configuration information, refer to the "Configuring IP Security Options" chapter in the *Security Configuration Guide*.

dnsix-dmdp retries

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** global configuration command. Use the **no** form of this command to restore the default number of retries.

```
dnsix-dmdp retries count  
no dnsix-dmdp retries count
```

Syntax Description

<i>count</i>	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.
--------------	--

Default

Retransmits messages up to 4 times, or until acknowledged

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands

```
dnsix-nat authorized-redirect  
dnsix-nat primary  
dnsix-nat secondary  
dnsix-nat source  
dnsix-nat transmit-count
```

dnsix-nat authorized-redirect

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirect** global configuration command. Use the **no** form of this command to delete an address.

```
dnsix-nat authorized-redirect ip-address  
no dnsix-nat authorized-redirect ip-address
```

Syntax Description

<i>ip-address</i>	IP address of the host from which redirection requests are permitted.
-------------------	---

Default

An empty list of addresses

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use multiple **dnsix-nat authorized-redirect** commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

Example

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1.

```
dnsix-nat authorization-redirect 192.168.1.1.
```

dnsix-nat primary

To specify the IP address of the host to which DNSIX audit messages are sent, use the **dnsix-nat primary** global configuration command. Use the **no** form of this command to delete an entry.

```
dnsix-nat primary ip-address  
no dnsix-nat primary ip-address
```

Syntax Description

ip-address IP address for the primary collection center.

Default

Messages are not sent.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

An IP address must be configured before audit messages can be sent.

Example

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.1.1.1
```

dnsix-nat secondary

To specify an alternate IP address for the host to which DNSIX audit messages are sent, use the **dnsix-nat secondary** global configuration command. Use the **no** form of this command to delete an entry.

```
dnsix-nat secondary ip-address  
no dnsix-nat secondary ip-address
```

Syntax Description

ip-address IP address for the secondary collection center.

Default

No alternate IP address is known.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Example

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To start the audit-writing module and to define audit trail source address, use the **dnsix-nat source** global configuration command. Use the **no** form of this command to disable the DNSIX audit trail writing module.

```
dnsix-nat source ip-address  
no dnsix-nat source ip-address
```

Syntax Description

ip-address Source IP address for DNSIX audit messages.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You must issue the **dnsix-nat source** command before any of the other **dnsix-nat** commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

Example

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0.

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

dnsix-nat transmit-count

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** global configuration command. Use the **no** form of this command to revert to the default audit message count.

```
dnsix-nat transmit-count count
no dnsix-nat transmit-count count
```

Syntax Description

<i>count</i>	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.
--------------	---

Default

One message is sent at a time.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Example

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

ip security add

To add a basic security option to all outgoing packets, use the **ip security add** interface configuration command. Use the **no** form of this command to disable the adding of a basic security option to all outgoing packets.

```
ip security add
no ip security add
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is enabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If an outgoing packet does not have a security option present, this interface configuration command will add one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the router. Because this action is performed after all the security tests have been passed, this label will either be the same or will fall within the range of the interface.

Example

The following example adds a basic security option to each packet leaving Ethernet interface 0:

```
interface ethernet 0
 ip security add
```

Related Commands

```
ip security dedicated
ip security extended-allowed
ip security first
ip security ignore-authorities
```

```
ip security implicit-labelling
ip security multilevel
ip security reserved-allowed
ip security strip
```

ip security aeso

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the `ip security aeso` interface configuration command. Use the `no` form of this command to disable AESO on an interface.

```
ip security aeso source compartment-bits
no ip security aeso source compartment-bits
```

Syntax Description

<i>source</i>	Extended Security Option (ESO) source. This can be an integer from 0 to 255.
<i>compartment-bits</i>	Compartment bits in hexadecimal.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Compartment bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.

Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.

Configuring any per-interface extended IP security option (IPSO) information automatically enables `ip security extended-allowed` (disabled by default).

Example

The following example defines the extended security option source as 5 and sets the compartments bits to 5:

```
interface ethernet 0
 ip security aeso 5 5
```

Related Commands

```
ip security eso-info
ip security eso-max
ip security eso-min
ip security extended-allowed
```

ip security dedicated

To set the level of classification and authority on the interface, use the `ip security dedicated` interface configuration command. Use the `no` form of this command to reset the interface to the default classification and authorities.

```
ip security dedicated level authority [authority...]
no ip security dedicated level authority [authority...]
```

Syntax Description

<i>level</i>	Degree of sensitivity of information. The level keywords are listed in Table 1.
<i>authority</i>	Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in Table 2.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving via this interface will have this label attached to it.

The following definitions apply to the descriptions of the IP security options (IPSO) in this section:

- level**—The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in Table 1.

Table 1 IPSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010

Table 1 IPSO Level Keywords and Bit Patterns (continued)

Level Keyword	Bit Pattern
Confidential	1001 0110
Reserved3	0110 0110
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

- **authority**—An organization that defines the set of security levels that will be used in a network. For example, the Genser authority consists of level names defined by the U.S. Defense Communications Agency (DCA). The authority keywords and their corresponding bit patterns are shown in Table 2.

Table 2 IPSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

- **label**—A combination of a security level and an authority or authorities.

Example

The following example sets a confidential level with Genser authority:

```
ip security dedicated confidential Genser
```

Related Commands

```
ip security add
ip security extended-allowed
ip security first
ip security ignore-authorities
ip security implicit-labelling
ip security multilevel
ip security reserved-allowed
ip security strip
```

ip security eso-info

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the `ip security eso-info` global configuration command. Use the `no` form of this command to return to the default settings.

```
ip security eso-info source compartment-size default-bit
no ip security eso-info source compartment-size default-bit
```

Syntax Description

<i>source</i>	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.
<i>compartment-size</i>	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.
<i>default-bit</i>	Default bit value for any unsent compartment bits.

Default

Disabled

Command mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command configures Extended Security Option (ESO) information, including Auxiliary Extended Security Option (AESO). Transmitted compartment info is padded to the size specified by the *compartment-size* argument.

Example

The following example sets system-wide defaults for source, compartment size, and the default bit value:

```
ip security eso-info 100 5 1
```

Related Commands

```
ip security eso-max  
ip security eso-min
```

ip security eso-max

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** interface configuration command. Use the **no** form of this command to return to the default.

```
ip security eso-max source compartment-bits  
no ip security eso-max source compartment-bits
```

Syntax Description

<i>source</i>	Extended Security Option (ESO) source. This is an integer from 1 to 255.
<i>compartment-bits</i>	Compartment bits in hexadecimal.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The command is used to specify the maximum sensitivity level for a particular interface. Before the per interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on the interface, these extended security options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Example

In the following example, the specified ESO source is 240 and the compartment bits are specified as 500:

```
interface ethernet 0
 ip security eso-max 240 500
```

Related Commands

ip security eso-info
ip security eso-min

ip security eso-min

To configure the minimum sensitivity for an interface, use the **ip security eso-min** interface configuration command. Use the **no** form of this command to return to the default.

```
ip security eso-min source compartment-bits
no ip security eso-min source compartment-bits
```

Syntax Description

<i>source</i>	Extended Security Option (ESO) source. This is an integer from 1 to 255.
<i>compartment-bits</i>	Compartment bits in hexadecimal.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The command is used to specify the minimum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on this interface, these extended security options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Example

In the following example, the specified ESO source is 5 and the compartment bits are specified as 5:

```
interface ethernet 0
 ip security eso-min 5 5
```

Related Commands

```
ip security eso-info
ip security eso-max
```

ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the `ip security extended-allowed` interface configuration command. Use the `no` form of this command to restore the default.

```
ip security extended-allowed
no ip security extended-allowed
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.
Packets containing extended security options are rejected.

Example

The following example allows interface Ethernet 0 to accept packets that have an extended security option present:

```
interface ethernet 0
 ip security extended-allowed
```

Related Commands

```
ip security add
ip security dedicated
ip security first
ip security ignore-authorities
ip security implicit-labelling
ip security multilevel
ip security reserved-allowed
ip security strip
```

ip security first

To prioritize the presence of security options on a packet, use the `ip security first` interface configuration command. Use the `no` form of this command to not move packets that include security options to the front of the options field.

```
ip security first
no ip security first
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If a basic security option is present on an outgoing packet, but it is not the first IP option, then the packet is moved to the front of the options field when this interface configuration command is used.

Example

The following example ensures that, if a basic security option is present in the options field of a packet exiting interface Ethernet 0, the packet is moved to the front of the options field:

```
interface ethernet 0
 ip security first
```

Related Commands

```
ip security add
ip security dedicated
ip security extended-allowed
ip security ignore-authorities
ip security implicit-labelling
ip security multilevel
ip security reserved-allowed
ip security strip
```

ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the `ip security ignore-authorities` interface configuration command. Use the `no` form of this command to disable this function.

```
ip security ignore-authorities
no ip security ignore-authorities
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

When the packet's authority field is ignored, the value used in place of this field is the authority value declared for the specified interface. The `ip security ignore-authorities` can only be configured on interfaces with dedicated security levels.

Example

The following example causes interface Ethernet 0 to ignore the authorities field on all incoming packets:

```
interface ethernet 0
 ip security ignore-authorities
```

Related Commands

```
ip security add
ip security dedicated
ip security extended-allowed
ip security first
ip security implicit-labelling
ip security multilevel
ip security reserved-allowed
ip security strip
```

ip security implicit-labelling

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the `ip security implicit-labelling` interface configuration command. Use the `no` form of this command to require security options.

```
ip security implicit-labelling [level authority [authority...]]
no ip security implicit-labelling [level authority [authority...]]
```

Syntax Description

<i>level</i>	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the <i>level</i> keywords listed in Table 1 in the <code>ip security dedicated</code> command section.)
<i>authority</i>	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the <i>authority</i> keywords listed in Table 2 in the <code>ip security dedicated</code> command section.)

Default

Enabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If your interface has multilevel security set, you must use the expanded form of the command (with the optional arguments as noted in brackets) because the arguments are used to specify the precise level and authority to use when labeling the packet. If your interface has dedicated security set, the additional arguments are ignored.

Example

In the following example, an interface is set for security and will accept unlabeled packets:

```
ip security dedicated confidential genser
ip security implicit-labelling
```

Related Commands

```
ip security add
ip security dedicated
ip security extended-allowed
ip security first
```

ip security ignore-authorities
ip security multilevel
ip security reserved-allowed
ip security strip

ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** interface configuration command. Use the **no** form of this command to remove security classifications and authorities.

```
ip security multilevel level1 [authority1...] to level2 authority2 [authority2...]  
no ip security multilevel
```

Syntax Description

<i>level1</i>	Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the <i>level</i> keywords found in Table 1 in the ip security dedicated command section.)
<i>authority1</i>	(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the <i>authority</i> keywords listed in Table 2 in the ip security dedicated command section.)
to	Separates the range of classifications and authorities.
<i>level2</i>	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the <i>level</i> keywords found in Table 1 in the ip security dedicated command section.)
<i>authority2</i>	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the <i>authority</i> keywords listed in Table 2 in the ip security dedicated command section.)

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

All traffic entering or leaving the system must have a security option that falls within this range. Being within range requires that the following two conditions be met:

- The classification level must be greater than or equal to *level1* and less than or equal to *level2*.
- The authority bits must be a superset of *authority1* and a proper subset of *authority2*. That is, *authority1* specifies those authority bits that are required on a packet, while *authority2* specifies the required bits plus any optional authorities that also can be included. If the *authority1* field is the empty set, then a packet is required to specify any one or more of the authority bits in *authority2*.

Example

The following example specifies levels Unclassified to Secret and NSA authority:

```
ip security multilevel unclassified to secret nsa
```

Related Commands

```
ip security add  
ip security dedicated  
ip security extended-allowed  
ip security first  
ip security ignore-authorities  
ip security implicit-labelling  
ip security reserved-allowed  
ip security strip
```

ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the `ip security reserved-allowed` interface configuration command. Use the `no` form of this command to not allow packets that have security levels of Reserved3 and Reserved2.

```
ip security reserved-allowed  
no ip security reserved-allowed
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

When you set multilevel security on an interface, and indicate, for example, that the highest range allowed is Confidential, and the lowest is Unclassified, the Cisco IOS software neither allows nor operates on packets that have security levels of Reserved3 and Reserved2 because they are undefined.

If you use the IP Security Option (IPSO) to block transmission out of unclassified interfaces, and you use one of the Reserved security levels, you *must* enable this feature to preserve network security.

Example

The following example allows a security level of Reserved through Ethernet interface 0:

```
interface ethernet 0
 ip security reserved-allowed
```

Related Commands

- ip security add
- ip security dedicated
- ip security extended-allowed
- ip security first
- ip security ignore-authorities
- ip security implicit-labelling
- ip security multilevel
- ip security strip

ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** interface configuration command. Use the **no** form of this command to restore security options.

```
ip security strip
no ip security strip
```

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The removal procedure is performed after all security tests in the router have been passed. This command is not allowed for multilevel interfaces.

Example

The following example removes any basic security options on outgoing packets on Ethernet interface 0:

```
interface ethernet 0
 ip security strip
```

Related Commands

- ip security add
- ip security dedicated
- ip security extended-allowed
- ip security first
- ip security ignore-authorities
- ip security implicit-labelling
- ip security multilevel
- ip security reserved-allowed

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the `show dnsix` privileged EXEC command.

```
show dnsix
```

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

The following is sample output from the `show dnsix` command:

```
Router# show dnsix

Audit Trail Enabled with Source 192.168.2.5
  State: PRIMARY
  Connected to 192.168.2.4
  Primary 192.168.2.4
  Transmit Count 1
  DMMP retries 4
  Authorization Redirection List:
    192.168.2.4
  Record count: 0
  Packet Count: 0
  Redirect Rcv: 0
```

