

Security Commands

- all-auto-sig-tunnels, on page 1
- authentication event fail, on page 2
- authentication event no-response action, on page 3
- authentication event server dead action authorize, on page 3
- authentication host-mode, on page 4
- aaa authentication dot1x, on page 5
- authentication open, on page 5
- authentication order, on page 6
- authentication port-control, on page 6
- authentication timer inactivity, on page 7
- authentication timer reauthenticate, on page 7
- authentication-type (security ipsec), on page 8
- dot1x pae, on page 9
- dot1x system-auth-control, on page 10
- extended-ar-window, on page 10
- ip access-group, on page 11
- ipsec (security), on page 11
- ip scp server enable, on page 12
- pairwise-keying (security ipsec), on page 13
- pwk-sym-rekey (security ipsec), on page 13
- rekey (security ipsec), on page 14
- replay-window (security ipsec), on page 14
- security, on page 15
- security ipsec integrity-type, on page 15
- sig-tunnel-list, on page 16
- switchport port-security, on page 17
- switchport port-security mac-address sticky, on page 18

all-auto-sig-tunnels

To start probe on all auto SIG active tunnels, use the **all-auto-sig-tunnels** in global configuration mode. To disable probing on all auto SIG active tunnels, use the **no** form of this command.

all-auto-sig-tunnels

no all-auto-sig-tunnels

Syntax Description This command has no arguments or keywords.

Command Modes global configuration mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **all-auto-sig-tunnels** to enable the CXP probes in all the active auto SIG tunnels configured in the node to select the best possible SIG tunnel for accessing the SaaS applications.

Examples The following example shows how to configure probing on all active auto SIG tunnels:

```
Device(config)# probe-path branch all-auto-sig-tunnels
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines For more information about this command, see the Cisco IOS XE authentication event fail command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
```

```
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication event no-response action

To specify how the Auth Manager handles authentication failures as a result of a nonresponsive host, use the **authentication event no-response action** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication event no-response action command.

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication event server dead action authorize command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

Supported Parameters

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication host-mode command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE aaa authentication dot1x command

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Device# config-transaction
Device(config)#aaa authentication dot1x default group radius none
```

authentication open

To allow a device to have network access via an interface without going through IEEE 802.1X authentication, use the **authentication open** command in the interface configuration mode. To disable open access for the interface, use the no form of the command.

authentication open

no authentication open

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE authentication open command.

Examples

The following example shows how to enable network access on a device without 802.1X authentication:

```
Device# config-transaction
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# authentication open
```

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

Supported Parameters

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication(MAB).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication order command.

authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

Supported Parameters

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication port-control command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
```

```
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity** command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

Supported Parameters

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication timer inactivity command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration or template configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

Supported Parameters

seconds	The number of seconds between reauthentication attempts. The range is from 1 to 65535. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE authentication timer reauthenticate command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

authentication-type (security ipsec)

To configure the type of authentication on IPsec tunnel connections between routers, use the **authentication-type** command in IPsec configuration mode. To delete the authentication type, use the no form of this command.

Note This command is not supported for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, use the **security ipsecintegrity-type** command instead.

authentication-type { **ah-no-id** | **ah-sha1-hmac** | **sha1-hmac** | **none** }

no authentication-type

Syntax Description

ah-no-id	Specifies a modified version of AH-SHA1 HMAC and ESP HMAC-SHA1 that ignores the ID field in the outer IP header of the packet.
sha1-hmac	Specifies ESP HMAC-SHA1. With this authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable).

ah-sha1-hmac	Specifies AH-SHA1 HMAC and ESP HMAC-SHA1. With the authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable).
none	Maps to no authentication. With this authentication type, ESP encrypts the inner header, packet payload, ESP trailer, and MPLS label (if applicable), but no HMAC-SHA1 hash is calculated.

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command is no longer supported. From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, use the **security ipsec integrity-type** command instead.

Examples

The following example shows how the router negotiates with the IPsec tunnel authentication types, AH-SHA1-HMAC, SHA1-HMAC, and AH-NO-ID:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# authentication-type sha1-hmac ah-sha1-hmac ah-no-id
```

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

Supported Parameters

authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE dot1x pae command.

Examples

```
interface {intf-name}
switchport mode access
switchport access vlan {vlan_id}
dot1x pae authenticator
authentication order dot1x mab
authentication host-mode single-host
```

```
authentication port-control auto
authentication timer reauthenticate <timer_num/server>
authentication timer inactivity <timer_num/server>
authentication event server dead action authorize vlan {critical_vlan}
authentication event fail action authorize vlan {restrict_vlan}
authentication event no-response action authorize vlan {guest_vlan}
no shutdown
```

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE dot1x system-auth-control command

Examples

The following example shows how to enable SystemAuthControl:

```
Device(config)# dot1x system-auth-control
```

extended-ar-window

To configure an extended anti-replay window, use the **extended-ar-window** command in the IPsec configuration mode. To remove the extended anti-replay window, use the **no** form of the command.

extended-ar-window *duration*

no extended-ar-window

Syntax Description

duration	Duration of the extended anti-replay window. Choose an appropriate duration based on the configured queue limits and the traffic profile. Default: 256 ms Range: 10ms to 2048ms

Command Default

By default, the extended anti-replay window is not configured.

Command Modes

IPsec configuration mode (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced.

Example

In the following example, an extended anti-replay window of 256ms is configured:

```
security
 ipsec
  extended-ar-window 256
```

ip access-group

To apply an IP access list to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list, use the **no** form of this command.

Supported Parameters

access-list-name	Name of the existing IP access list as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. • Integer from 1 to 199 for a standard or extended IP access list. • Integer from 1300 to 2699 for a standard or extended IP expanded access list.
out	Filters on outbound packets.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE ip access-group command.

Examples

```
ip access-group 1 out
ipv6 enable
keepalive 60
```

ipsec (security)

To configure the parameters for IPsec tunnel connections on routers, use the **ipsec** command in security configuration mode.

ipsec

Syntax Description

This command has no arguments or keywords.

Command Modes

security configuration (config-security)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to apply the IPsec rekeying interval, modify the size of IPsec replay window, and configure multiple authentication types:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# rekey 1209600
Router(config-ipsec)# replay-window 4096
Router(config-ipsec)# authentication-type ah-sha1-hmac ah-sha1-hmac ah-no-id
Router(config-ipsec)# pairwise-keying
```

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), use the **no** form of this command.

ip scp server enable
no ip scp server enable

Syntax Description

This command has no arguments or keywords.

Command Default

The secure copy function is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip scp server enable command.

Examples

The following example shows how to configure the router to allow the router to securely copy files from a remote workstation. AAA must be configured as scp relies on AAA authentication and authorization.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
```

```
username user1 privilege 15 password 0 lab
ip scp server enable
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
username	Establishes a username-based authentication system.

pairwise-keying (security ipsec)

To configure the private pairwise IPsec session keys for secure communication between IPsec routers and its peers, use the **pairwise-keying** command in IPsec configuration mode. To delete the pairwise IPsec session keys, use the no form of this command.

pairwise-keying

no pairwise-keying

Syntax Description

This command has no arguments or keywords.

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure a pair of IPsec session keys per pair of local and remote TLOC:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# authentication-type ah-sha1-hmac ah-sha1-hmac ah-no-id
Router(config-ipsec)# pairwise-keying
```

pwk-sym-rekey (security ipsec)

To enable symmetric rekeying when pairwise keying is enabled, use the **pwk-sym-rekey** in IPsec configuration mode. To disable symmetric rekeying, use the no form of this command.

pwk-sym-rekey

no pwk-sym-rekey

Syntax Description This command has no arguments or keywords.

Command Modes IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to configure rekeying for IPsec pairwise keys:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# pairwise-keying
Router(config-ipsec)# pwk-sym-rekey
```

rekey (security ipsec)

To modify the IPsec rekeying timer on routers, use the **rekey** command in IPsec configuration mode. To delete the rekey timer on routers, use the no form of this command.

rekey *time-interval*

no rekey

Syntax Description

time-interval	Specifies how often IKE changes the AES key that is used during IKE key exchanges. Range: 10 - 1209600 seconds (up to 14 days) Default: 86400 seconds

Command Modes IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples The following example shows how to change the rekeying interval for IKE key exchanges to 7 days:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# rekey 604800
```

replay-window (security ipsec)

To modify the size of the IPsec replay window on routers, use the **replay-window** command in IPsec configuration mode. To delete the replay window size on routers, use the no form of this command.

replay-window *replay-window-size*

no replay-window

Syntax Description

replay-window-size	Specifies the size of the sliding replay window method. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets Default: 512 packets

Command Modes

IPsec configuration (config-ipsec)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example changes the replay window size to 1024:

```
Router(config)# security
Router(config-security)# ipsec
Router(config-ipsec)# replay-window 1024
```

security

To configure security parameters on routers, Cisco vManage, and Cisco vSmart Controllers, use the **security** command in global configuration mode.

security

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure the security for a router.

```
Router(config)# security
```

security ipsec integrity-type

To configure the type of integrity check performed on IPSec packets, use the **security ipsec integrity-type** command in global configuration mode. To delete the authentication type, use the **no** form of this command.

security ipsec integrity-type { **none** | **ip-udp-esp** | **ip-udp-esp-no-id** | **esp** }

no security ipsec integrity-type

Syntax Description

none	This option turns integrity checking off on IPSec packets. We don't recommend using this option.
ip-udp-esp	Enables ESP encryption. In addition to the integrity checks on the Encapsulating Security Payload (ESP) header and payload, the checks also include the outer IP and UDP headers.
ip-udp-esp-no-id	This is similar to ip-udp-esp option, however, the ID field of the outer IP header is ignored. Configure this option in the list of integrity types to have the Cisco SD-WAN software ignore the ID field in the IP header so that the Cisco SD-WAN can work in conjunction with non-Cisco devices.
esp	Enables ESP encryption and integrity checking on ESP header.

Command Default

When an integrity-type is not specified, tbe default integrity-type is ip-udp-esp esp.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced. **Note** From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, this command replaces the **security ipsec authentication-type** command.

Usage Guidelines

Configure each integrity type separately using the **security ipsec integrity-type** command.

Example

This example shows how to configure the various integrity types that are supported.

```
Device(config)# security ipsec integrity-type ip-udp-esp
Device(config)# security ipsec integrity-type ip-udp-esp-no-id
Device(config)# security ipsec integrity-type esp
```

sig-tunnel-list

To configure the manual tunnels or a specific set of auto-tunnels for probing instead of all the auto-tunnels, use the **sig-tunnel-list** command in global configuration mode.

sig-tunnel-list *list of SIG tunnels*

no probe-path gateway sig-tunnel-list

Syntax Description

list of SIG tunnels	Specifies a specific set of auto-tunnels for probing.

Command Modes

global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example shows how to configure the manual tunnels or a specific set of auto-tunnels for probing instead of all the auto-tunnels:

```
Device(config)# probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
```

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security
no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE switchport port-security command.

Port security configuration is supported on Cisco ISR4000 and Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules.

Examples

The following example shows how to enable port security:

```
Device(config-if)# switchport port-security
```

The following example shows how to disable port security:

```
Device(config-if)# no switchport port-security
```

switchport port-security mac-address sticky

To configure the dynamic MAC addresses as sticky on an interface, use the **switchport port-security mac-address sticky** command. To disable the sticky feature on an interface, use the **no** form of this command.

switchport port-security mac-address sticky
no switchport port-security mac-address sticky

Syntax Description

sticky	Configures the dynamic MAC addresses as sticky on an interface. By default, sticky is disabled.

Command Default

MAC addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE switchport port-security mac-address command.

Port security configuration is supported on Cisco ISR4000 and Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules.

Examples

The following example shows how to enable the sticky feature on an interface:

```
Device(config-if)# switchport port-security mac-address sticky
```

The following example shows how to disable the sticky feature on an interface:

```
Device(config-if)# no switchport port-security mac-address sticky
```