CHAPTER 50

Configuring Auto Security

This chapter describes how to configure auto security on the Catalyst 4500 series switch.

It consists of these sections:

Note For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library. See the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

About Auto Security

Prior to Release IOS XE 3.6.0E and IOS 15.2(2)E, the Catalyst 4500 series switch offered IPv4 baseline security features (like Port Security), which must be enabled globally and on per port basis. Moreover, the baseline security feature CLIs for uplink ports differ from those for downlink CLIs.

Beginning with Release IOS XE 3.6.0E and IOS 15.2(2)E, the Catalyst 4500 series switch supports Auto Security (AS), which provides a single line CLI, to enable base line security features.

AS supports the IPv4 baseline security features: DHCP Snooping, Dynamic ARP Inspection, and Port Security.

Feature Interaction

Auto security interacts with Port Security, DHCP snooping, DAI modules.

DHCP Snooping

Auto Security (AS) enables DHCP Snooping globally (with the **ip dhcp snooping** command) and also on VLANs 2-1005 (with the **ip dhcp snooping vlan** *vlanid* command).

AS configures trunk or DHCP server-facing port(s) as trusted (with the **ip dhcp-snooping trust** command).

Dynamic ARP Inspection

AS enables this feature globally on all VLANs present on the switch (with the **ip arp inspection vlan** *vlanid*) command.

AS configures the trunk port as trusted (with the **ip arp inspection trust** command).

Port Security

AS enables this feature on all the switch's access ports (with the **switchport port-security** command).]

Configuring Auto Security

Enabling auto security globally

To enable auto security globally, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# auto security`	Enables auto security globally.
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show running-config | i security`	(Optional) Saves your entries in the configuration file.

This example shows how to enable auto security globally:

```
Switch(config)# auto security
Switch# show running-config | i security
auto security
```

Relevant baseline security feature CLI as shown in the output of the show auto security command is applied on or removed from access and trunk ports.

Disabling auto security globally

To disable auto security globally, perform this task:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# no auto security`	Dis-enables auto security globally.
Step 3	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 4	`Switch# show running-config | isecurity`	(Optional) Saves your entries in the configuration file.

This example show how to dis-enable auto security globally:

```
Switch(config)# no auto security
Switch# show auto security
Auto Security is Disabled globally

AutoSecure is Enabled on below interface(s):
-------------------------------------------

Switch#
```

Enabling Auto Security Feature for Access (End Hosts) or Trunk (Uplink) Ports

Use the a**uto security-port** [**host** | **uplink**] command, to enable auto security for access (end hosts) and uplink ports:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface` *interface*	Enters interface mode
Step 3	`Switch(config-if)# auto security-port` [**host** | **uplink**]	Enables auto security on host or uplink ports.
Step 4	`Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# show auto security`	Displays the status of auto security.

This example displays how to enable auto security for an uplink port:

This example shows how to configure a port as auto security-port uplink.

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int g1/0/15
Switch(config-if)# switchport mode trunk
Switch(config-if)# auto security-port uplink
Switch(config-if)# end
```

Use the **show auto security** and **show running-config** commands confirm the prior configuration.

```
Switch# show auto security
Auto Security is Enabled globally

AutoSecure is Enabled on below interface(s):
-------------------------------------------
```

```
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/15

Switch# show running-config int g1/0/15
Building configuration...

Current configuration : 127 bytes
!
interface GigabitEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 auto security-port uplink
end
```

This example shows how to configure a port as an auto-security port host.

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int g1/0/18
Switch(config-if)# switchport mode access
Switch(config-if)# auto security-port host
Switch(config-if)# end
Switch#

Use the auto security and show running-config commands to confirm the prior configuration.

Switch# show auto security
Auto Security is Enabled globally

AutoSecure is Enabled on below interface(s):
-------------------------------------------
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/15
   GigabitEthernet1/0/18

Switch# show run int g1/0/18
Building configuration...

Current configuration : 165 bytes
!
interface GigabitEthernet1/0/18
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 40
 auto security-port host
 spanning-tree portfast
```

Disabling Auto Security Feature for Access (End Hosts) or Uplink Ports

Use the **no auto security-port** command to disable auto security on a port:

	Command	Purpose
Step 1	`Switch# configure terminal`	Enters global configuration mode.
Step 2	`Switch(config)# interface interface`	Enters interface mode
Step 3	`Switch(config-if)# no auto security-port`	Disables auto security on a port.
Step 4	`Switch(config-if)# end`	Exits to EXEC mode.

	Command	Purpose
Step 5	`Switch(config)# do show run int` *`interface`*	Verifies auto security-port being disabled.
Step 6	`Switch(config)# end`	Returns to privileged EXEC mode.

This example shows how to disable auto security:

```
Switch# show run int g1/0/15
Building configuration...

Current configuration : 137 bytes
!
interface GigabitEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 auto security-port uplink
end
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int g1/0/15
Switch(config-if)# no auto security-port
Switch(config-if)# end
Switch# show run int g1/0/15
Building configuration...

Current configuration : 110 bytes
!
interface GigabitEthernet1/0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

show command

Use the **show auto security** command, verify the status of auto-security on the interface and global level.

Use the **show auto security** [**configuration**] command, to view the CLIs that are applied with AS.

This example shows the output of the **show auto security** command when AS is enabled:

```
Switch# show auto security
Auto Security is Enabled globally
AutoSecurity is Enabled on below interface(s):
-------------------------------------------
   GigabitEthernet2/0/2
   GigabitEthernet2/0/3
   GigabitEthernet2/0/4
   GigabitEthernet2/0/5
   GigabitEthernet2/0/6
   GigabitEthernet2/0/7
   GigabitEthernet2/0/8
   GigabitEthernet2/0/9
```

This example shows the output of the **show auto security configuration** command when AS is enabled:

```
Switch# show auto security configuration
%AutoSecurity provides a single CLI config 'auto security'
 to enable Base-line security Features like
 DHCP snooping, ARP inspection and Port-Security
Auto Security CLIs applied globally:
-----------------------------------
ip dhcp snooping
```

```
ip dhcp snooping vlan 2-1005
no ip dhcp snooping information option
ip arp inspection vlan 2-1005
ip arp inspection validate src-mac dst-mac ip

Auto Security CLIs applied on Access Port:
------------------------------------------
switchport port-security
switchport port-security maximum 2
switchport port-security maximum vlan access 1
switchport port-security maximum vlan voice 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
ip arp inspection limit rate 100
ip dhcp snooping limit rate 100


Auto Security CLIs applied on Trunk Port:
-----------------------------------------
ip dhcp snooping trust
ip arp inspection trust
switchport port-security
switchport port-security maximum 100
switchport port-security violation restrict
```

Sample Output when Auto Security is Enabled

This example shows the output of the **show auto security** command when AS is enabled:

```
Switch# show auto security
Auto Security is Enabled globally

AutoSecure is Enabled on below interface(s):
--------------------------------------------
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/14
```

Sample Output when Auto Security is Disabled

This example shows the output of the **show auto security** command when AS is disabled:

```
Switch# show auto security
Auto Security is Disabled globally

AutoSecure is Enabled on below interface(s):
--------------------------------------------
  none
Switch#
```

Guidelines and Restrictions

- The **auto security** command has no parameters.
- Base line security CLIs (like port security) are not individually nvgen'd on interfaces that have auto security-port configured. This allows you to maintain consistency over reboots.
- After auto security-port is enabled on a port, you cannot change the CLIs of the baseline security features (Port Security, DAI, and DHCP Snooping).

For example, if you enter the following:

```
interface GigabitEthernet2/0/24
switchport mode access
auto security-port  host
```

The port security configuration is rejected on the auto security port:

```
Switch(config)# int g2/0/24
Switch(config-if)# switchport port-security maximum 4
%Command Rejected: 'auto security' enabled port
```

- Because you might need a different set of features on uplink ports, such as marking the port as a DHCP trusted port, you need to identify uplink and downlink ports and apply port mode specific configuration.
  - Starting with Cisco IOS XE 3.6.0E (IOS 15.2.(2)E), all trunk ports are treated as uplink ports and all access port are treated as host ports.
  - AS assumes that you will configure the port with data and voice VLANs.
  - AS is not supported on routed or Layer 3 ports, dynamic ports, or VSL links.
- Enabling auto security should elicit system confirmation because the current baseline security configuration will be removed as the auto security configuration is applied. When auto security is globally enabled, existing configurations related to DAI, DHCP, and PSEC are removed and security violation may be triggered on the auto-security enabled port when incoming MACs exceed the limit.

  When we issue **auto security** in global or interface config mode, any baseline security configuration on the interfaces or on the switch is removed and auto security configuration is applied. Disabling auto security does not restore the previous security configuration.