



## CHAPTER 10

# Configuring Port Security

---

This chapter describes how to configure port security on NX-OS devices.

This chapter includes the following sections:

- [Information About Port Security, page 10-1](#)
- [Licensing Requirements for Port Security, page 10-6](#)
- [Prerequisites for Port Security, page 10-6](#)
- [Guidelines and Limitations, page 10-7](#)
- [Configuring Port Security, page 10-7](#)
- [Displaying Secure MAC Addresses, page 10-15](#)
- [Displaying Violation Statistics, page 10-16](#)
- [Field Descriptions for Port Security, page 10-16](#)
- [Additional References, page 10-18](#)

## Information About Port Security

Port security allows you to configure Layer 2 interfaces that allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.

This section includes the following topics:

- [Secure MAC Address Learning, page 10-2](#)
- [Dynamic Address Aging, page 10-3](#)
- [Secure MAC Address Maximums, page 10-3](#)
- [Security Violations and Actions, page 10-4](#)
- [Port Security and Port Types, page 10-5](#)
- [Port Type Changes, page 10-5](#)
- [802.1X and Port Security, page 10-5](#)
- [Virtualization Support, page 10-6](#)

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Secure MAC Address Learning

The process of securing a MAC address is called learning. The number of addresses that can be learned is restricted, as described in the [“Secure MAC Address Maximums” section on page 10-3](#). For each interface that you enable port security on, the device can learn addresses by the static, dynamic, or sticky methods.

### Static Method

The static learning method allows you to manually add or remove secure MAC addresses to the configuration of an interface.

A static secure MAC address entry remains in the configuration of an interface until one of the following events occurs:

- You explicitly remove the address from the configuration. For more information, see the [“Removing a Static Secure MAC Address on an Interface” section on page 10-12](#).
- You configure the interface to act as a Layer 3 interface. For more information, see the [“Port Type Changes” section on page 10-5](#).

Adding secure addresses by the static method is not affected by whether dynamic or sticky address learning is enabled.

### Dynamic Method

By default, when you enable port security on an interface, you enable the dynamic learning method. With this method, the device secures MAC addresses as ingress traffic passes through the interface. If the address is not yet secured and the device has not reached any applicable maximum, it secures the address and allows the traffic.

The device ages dynamic addresses and drops them once the age limit is reached, as described in the [“Dynamic Address Aging” section on page 10-3](#).

Dynamic addresses do not persist through a device restart or through restarting the interface.

To remove a specific address learned by the dynamic method or to remove all addresses learned by the dynamic method on a specific interface, see the [“Removing a Dynamic or Sticky Secure MAC Address” section on page 10-12](#).

### Sticky Method

If you enable the sticky method, the device secures MAC addresses in the same manner as dynamic address learning, but the device stores addresses learned by this method in non-volatile RAM (NVRAM). As a result, addresses learned by the sticky method persist through a device restart. Sticky secure MAC addresses do not appear in the running configuration of an interface.

Dynamic and sticky address learning are mutually exclusive. When you enable sticky learning on an interface, the device stops dynamic learning and performs sticky learning instead. If you disable sticky learning, the device resumes dynamic learning.

The device does not age sticky secure MAC addresses.

To remove a specific address learned by the sticky method, see the [“Removing a Static Secure MAC Address on an Interface” section on page 10-12](#).

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Dynamic Address Aging

The device ages MAC addresses learned by the dynamic method and drops them after the age limit is reached. You can configure the age limit on each interface. The range is from 0 to 1440 minutes, where 0 disables aging.

The method that the device uses to determine that the MAC address age is also configurable. The two methods of determining address age are as follows:

- Inactivity—The length of time after the device last received a packet from the address on the applicable interface.
- Absolute—The length of time after the device learned the address. This is the default aging method; however, the default aging time is 0 minutes, which disables aging.

## Secure MAC Address Maximums

By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static.



**Tip**

---

To ensure that an attached device has the full bandwidth of the port, set the maximum number of addresses to one and configure the MAC address of the attached device.

---

The following three limits can determine how many secure MAC address are permitted on an interface:

- Device maximum—The device has a nonconfigurable limit of 8192 secure MAC addresses. If learning a new address would violate the device maximum, the device does not permit the new address to be learned, even if the interface or VLAN maximum has not been reached.
- Interface maximum—You can configure a maximum number of secure MAC addresses for each interface protected by port security. The default interface maximum is one address. Interface maximums cannot exceed the device maximum.
- VLAN maximum—You can configure the maximum number of secure MAC addresses per VLAN for each interface protected by port security. A VLAN maximum cannot exceed the interface maximum. VLAN maximums are useful only for trunk ports. There are no default VLAN maximums.

For an example of how VLAN and interface maximums interact, see the [“Security Violations and Actions”](#) section on page 10-4.

You can configure VLAN and interface maximums per interface, as needed; however, when the new limit is less than the applicable number of secure addresses, you must reduce the number of secure MAC addresses first. To remove dynamically learned addresses, see the [“Removing a Dynamic or Sticky Secure MAC Address”](#) section on page 10-12. To remove addresses learned by the sticky or static methods, see the [“Removing a Static Secure MAC Address on an Interface”](#) section on page 10-12.

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

## Security Violations and Actions

Port security triggers security violations when either of the two following events occur:

- Ingress traffic arrives at an interface from a nonsecure MAC address and learning the address would exceed the applicable maximum number of secure MAC addresses.

When an interface has both a VLAN maximum and an interface maximum configured, a violation occurs when either maximum is exceeded. For example, consider the following on a single interface configured with port security:

- VLAN 1 has a maximum of 5 addresses
- The interface has a maximum of 10 addresses

The device detects a violation when any of the following occurs:

- The device has learned five addresses for VLAN 1 and inbound traffic from a sixth address arrives at the interface in VLAN 1.
- The device has learned 10 addresses on the interface and inbound traffic from an 11th address arrives at the interface.
- Ingress traffic from a secure MAC address arrives at a different interface in the same VLAN as the interface on which the address is secured.



### Note

---

After a secure MAC address is configured or learned on one secure port, the sequence of events that occurs when port security detects that secure MAC address on a different port in the same VLAN is known as a MAC move violation.

---

When a security violation occurs, the device takes the action specified by the port security configuration of the applicable interface. The possible actions that the device can take are as follows:

- Shutdown—Shuts down the interface that received the packet triggering the violation. The interface is error disabled. This action is the default. After you reenables the interface, it retains its port security configuration, including its secure MAC addresses.
- Restrict—Drops ingress traffic from any nonsecure MAC addresses. The device keeps a count of the number of dropped packets.
- Protect—Prevents violations from occurring. Address learning continues until the maximum number of MAC addresses on the interface is reached, after which the device disables learning on the interface and drops all ingress traffic from nonsecure MAC addresses.

If a violation occurs because ingress traffic from a secure MAC address arrives at a different interface than the interface on which the address is secure, the device applies the action on the interface that received the traffic.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## Port Security and Port Types

You can configure port security only on Layer 2 interfaces. Details about port security and different types of interfaces or ports are as follows:

- Access ports—You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN.
- Trunk ports—You can configure port security on interfaces that you have configured as Layer 2 trunk ports. VLAN maximums are not useful for access ports. The device allows VLAN maximums only for VLANs associated with the trunk port.
- SPAN ports—You can configure port security on SPAN source ports but not on SPAN destination ports.
- Ethernet Port Channels—Port security is not supported on Ethernet port channels.

## Port Type Changes

When you have configured port security on a Layer 2 interface and you change the port type of the interface, the device behaves as follows:

- Access port to trunk port—When you change a Layer 2 interface from an access port to a trunk port, the device drops all secure addresses learned by the dynamic method. The device moves the addresses learned by the static or sticky method to the native trunk VLAN.
- Trunk port to access port—When you change a Layer 2 interface from a trunk port to an access port, the device drops all secure addresses learned by the dynamic method. It also moves all addresses learned by the sticky method on the native trunk VLAN to the access VLAN. The device drops secure addresses learned by the sticky method if they are not on the native trunk VLAN.
- Switched port to routed port—When you change an interface from a Layer 2 interface to a Layer 3 interface, the device disables port security on the interface and discards all port security configuration for the interface. The device also discards all secure MAC addresses for the interface, regardless of the method used to learn the address.
- Routed port to switched port—When you change an interface from a Layer 3 interface to a Layer 2 interface, the device has no port security configuration for the interface.

## 802.1X and Port Security

You can configure port security and 802.1X on the same interfaces. Port security secures the MAC addresses that 802.1X authenticates. 802.1X processes packets before port security processes them, so when you enable both on an interface, 802.1X is already preventing inbound traffic on the interface from unknown MAC addresses.

When you enable 802.1X and port security on the same interface, port security continues to learn MAC addresses by the sticky or dynamic method, as configured. Additionally, depending on whether you enable 802.1X in single-host mode or multiple-host mode, one of the following occurs:

- Single host mode—Port security learns the MAC address of the authenticated host.
- Multiple host mode—Port security drops any MAC addresses learned for this interface by the dynamic method and learns the MAC address of the first host authenticated by 802.1X.

If a MAC address that 802.1X passes to port security would violate the applicable maximum number of secure MAC addresses, the device sends an authentication failure message to the host.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

The device treats MAC addresses authenticated by 802.1X as though they were learned by the dynamic method, even if port security previously learned the address by the sticky or static methods. If you attempt to delete a secure MAC address that has been authenticated by 802.1X, the address remains secure.

If the MAC address of an authenticated host is secured by the sticky or static method, the device treats the address as if it were learned by the dynamic method, and you cannot delete the MAC address manually.

Port security integrates with 802.1X to reauthenticate hosts when the authenticated and secure MAC address of the host reaches its port security age limit. The device behaves differently depending upon the type of aging, as follows:

- **Absolute**—Port security notifies 802.1X and the device attempts to reauthenticate the host. The result of reauthentication determines whether the address remains secure. If reauthentication succeeds, the device restarts the aging timer on the secure address; otherwise, the device drops the address from the list of secure addressees for the interface.
- **Inactivity**—Port security drops the secure address from the list of secure addresses for the interface and notifies 802.1X. The device attempts to reauthenticate the host. If reauthentication succeeds, port security secures the address again.

## Virtualization Support

Port security supports VDCs as follows:

- Port security is local to each VDC. You enable and configure port security on a per-VDC basis.
- Each VDC maintains secure MAC addresses separately.
- The device cannot issue a security violation when a secured MAC address in one VDC is seen on a protected interface in another VDC.

## Licensing Requirements for Port Security

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Port security requires a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the <i>Cisco DCNM Licensing Guide</i> .
NX-OS	Port security requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS device images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</i> .

## Prerequisites for Port Security

Port security has the following prerequisites:

- You must globally enable port security for the device that you want to protect with port security.

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Guidelines and Limitations

When configuring port security, follow these guidelines:

- Port security does not support Ethernet port-channel interfaces or switched port analyzer (SPAN) destination ports.
- Port security does not depend upon other features.
- Port security can work with 802.1X, as described in the “802.1X and Port Security” section on page 10-5.
- For each device that you use DCCM to configure port security, ensure that you configure the logging level for port security to 5 (Notifications) or a higher level. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

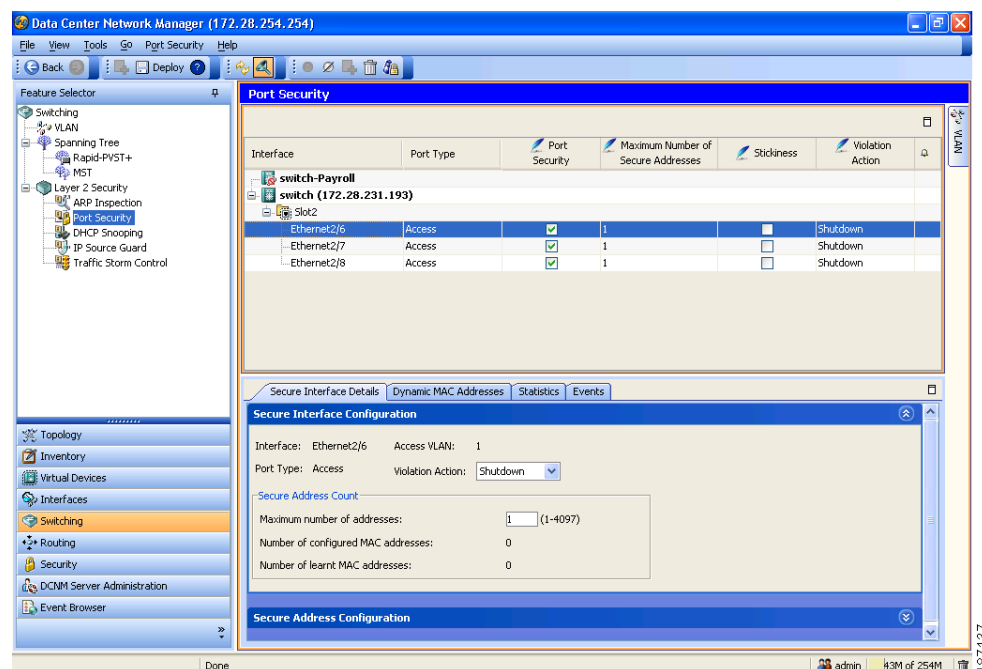
```
switch(config)# logging level port-security 5
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about NX-OS system-message logging requirements, see the *Cisco DCCM Fundamentals Configuration Guide, Release 4.0*.

## Configuring Port Security

Figure 10-1 shows the Port Security content pane.

**Figure 10-1** Port Security Content Pane



This section includes the following topics:

- [Enabling or Disabling Port Security Globally, page 10-8](#)

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- [Enabling or Disabling Port Security on a Layer 2 Interface](#), page 10-9
- [Enabling or Disabling Sticky MAC Address Learning](#), page 10-10
- [Adding a Static Secure MAC Address on an Interface](#), page 10-10
- [Removing a Static Secure MAC Address on an Interface](#), page 10-12
- [Removing a Dynamic or Sticky Secure MAC Address](#), page 10-12
- [Configuring a Maximum Number of MAC Addresses](#), page 10-13
- [Configuring an Address Aging Type and Time](#), page 10-14
- [Configuring a Security Violation Action](#), page 10-14

## Enabling or Disabling Port Security Globally

You can enable or disable port security globally on a device.

When you disable port security globally, all port security configuration is lost, including any statically configured secure MAC addresses and all dynamic or sticky secured MAC addresses.

### BEFORE YOU BEGIN

By default, port security is disabled.

Ensure that you configure the logging level for port security to 5 (Informational) or a higher level on the NX-OS device. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level port-security 5
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0*.

### DETAILED STEPS

To enable or disable port security on a device, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, click the device on which you want to enable or disable port security.
- Step 3** Do one of the following:
- To enable port security globally on the device, from the menu bar, choose **Port Security > Enable Port Security**.  
The Stop Learning check box appears on the Global Settings tab in the Details pane.
  - To disable port security globally on the device, from the menu bar, choose **Port Security > Disable Port Security**.  
The “Port Security is disabled on device” message appears on the Global Settings tab in the Details pane.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.

---

## Enabling or Disabling Port Security on a Layer 2 Interface

You can enable or disable port security on a Layer 2 interface. For more information about dynamic learning of MAC addresses, see the [“Secure MAC Address Learning”](#) section on page 10-2.



### Note

You cannot enable port security on a routed interface.

---

### BEFORE YOU BEGIN

By default, port security is disabled on all interfaces.

Enabling port security on an interface also enables dynamic MAC address learning. If you want to enable sticky MAC address learning, you must also complete the steps in the [“Enabling or Disabling Sticky MAC Address Learning”](#) section on page 10-10.

Ensure that port security is enabled. To enable port security, see the [“Enabling or Disabling Port Security Globally”](#) section on page 10-8.

### DETAILED STEPS

To enable or disable port security on an interface, follow these steps:

---

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface on which you want to enable or disable port security.  
The Summary pane displays the slots on the device and any interfaces on which port security is configured. The slot remains selected.
- Step 3** (Optional) If the interface that you need does not appear, from the menu bar, choose **Port Security > Add Interface**. In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.  
The interface name appears in the new row of the Summary pane.
- Step 4** Click the interface on which you want to enable or disable port security.
- Step 5** Do one of the following:
- To enable port security on the selected interface, in the Port Security column, check the check box.  
Port security is enabled on the selected interface.
  - To disable port security on the selected interface, in the Port Security column, uncheck the check box.  
Port security is disabled on the selected interface.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Enabling or Disabling Sticky MAC Address Learning

You can disable or enable sticky MAC address learning on an interface. If you disable sticky learning, the device returns to dynamic MAC address learning on the interface, which is the default learning method.

### BEFORE YOU BEGIN

By default, sticky MAC address learning is disabled.

Ensure that port security is enabled globally and on the interface that you are configuring. To enable port security globally, see the [“Enabling or Disabling Port Security Globally”](#) section on page 10-8. To enable port security on the interface, see the [“Enabling or Disabling Port Security on a Layer 2 Interface”](#) section on page 10-9.

### DETAILED STEPS

To enable or disable sticky secure MAC address learning, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface on which you want to enable or disable port security.  
The slots on the device and any interfaces on which port security is configured appear in the Summary pane. The slot remains selected.
- Step 3** Click the interface on which you want to enable or disable sticky MAC address learning.
- Step 4** Do one of the following:
- To enable sticky MAC address learning on the selected interface, in the Stickiness column, check the check box.  
Sticky MAC address learning is enabled on the selected interface.
  - To disable sticky MAC address learning on the selected interface, in the Stickiness column, uncheck the check box.  
Sticky MAC address learning is disabled on the selected interface.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Adding a Static Secure MAC Address on an Interface

You can add a static secure MAC address on a Layer 2 interface. If the interface is in trunk port mode, you must assign the new static secure MAC address to a VLAN.

### BEFORE YOU BEGIN

By default, no static secure MAC addresses are configured on an interface.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

Determine if the interface maximum has been reached for secure MAC addresses (see the “[Displaying Secure MAC Addresses](#)” section on page 10-15). If needed, you can remove a secure MAC address (see the “[Removing a Static Secure MAC Address on an Interface](#)” section on page 10-12 or the “[Removing a Dynamic or Sticky Secure MAC Address](#)” section on page 10-12) or you can change the maximum number of addresses on the interface (see the “[Configuring a Maximum Number of MAC Addresses](#)” section on page 10-13).

Ensure that port security is enabled both globally and on the interface. To enable port security globally, see the “[Enabling or Disabling Port Security Globally](#)” section on page 10-8. To enable port security on the interface, see the “[Enabling or Disabling Port Security on a Layer 2 Interface](#)” section on page 10-9.

## DETAILED STEPS

To add a static secure MAC address on an interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface that you want to configure with a static secure MAC address.  
The slots on the device and any interfaces on which port security is configured appear in the Summary pane. The slot remains selected.
  - Step 3** Click the interface on which you want to configure an address.
  - Step 4** From the Details pane, click the **Secure Interface Details** tab.
  - Step 5** Expand the **Secure Address Configuration** section, if necessary.  
A table of secure MAC addresses appears in the Secure Address Configuration section. If the interface that you selected is in trunk port mode, the table is organized by VLAN ID.
  - Step 6** (Optional) If the interface is in trunk port mode and the VLAN for the new secure address does not appear, right-click either on an existing VLAN entry or on a blank row, choose **Add VLAN**, and then from the drop-down list, choose the VLAN ID that you need to associate the secure address with.  
The VLAN that you chose appears in the table on the Secure Address Configuration section.
  - Step 7** (Optional) If the interface is in trunk port mode, expand the VLAN that you need to add the secure address to.
  - Step 8** Under the Host MAC Address heading, right-click on a blank area and choose **Add Host**.  
A new row appears under the Host MAC Address heading.
  - Step 9** Double-click on the new row and enter the new static secure MAC address.
  - Step 10** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

*Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).*

## Removing a Static Secure MAC Address on an Interface

You can remove a static secure MAC address on a Layer 2 interface.

### BEFORE YOU BEGIN

Ensure that port security is enabled. To enable port security globally, see the “[Enabling or Disabling Port Security Globally](#)” section on page 10-8. To enable port security on the interface, see the “[Enabling or Disabling Port Security on a Layer 2 Interface](#)” section on page 10-9.

To remove a static secure MAC address from an interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface with a static secure MAC address that you want to delete.  
The slots on the device and any interfaces on which port security is configured appear in the Summary pane. The slot remains selected.
- Step 3** Click the interface from which you want to delete an address.
- Step 4** From the Details pane, click the **Secure Interface Details** tab.
- Step 5** If necessary, expand the **Secure Address Configuration** section.  
A table of secure MAC addresses appears in the Secure Address Configuration section. If the interface that you selected is in trunk port mode, the table is organized by VLAN ID.
- Step 6** (Optional) If the interface is in trunk port mode, expand the VLAN that you need to remove the secure address from.  
Secure MAC addresses associated with the selected VLAN appear in the table below the Host MAC Address heading.
- Step 7** Right-click the address that you need to remove and choose **Delete Host**.  
A confirmation warning appears.
- Step 8** Click **Yes**.  
The address disappears from the table of static secure MAC addresses.
- Step 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Removing a Dynamic or Sticky Secure MAC Address

You can remove dynamically learned, secure MAC addresses, including sticky secure MAC addresses.

### DETAILED STEPS

To remove a dynamic or static secure MAC address from an interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface with a dynamic or static secure MAC address that you want to delete.
- The slots on the device and any interfaces on which port security is configured appear in the Summary pane. The slot remains selected.
- Step 3** Click the interface from which you want to delete an address.
- Step 4** From the Details pane, click the **Dynamic MAC Addresses** tab.
- A table of dynamic secure MAC addresses, organized by VLAN ID, appears.
- Step 5** Right-click the address that you need to remove and choose **Clear MAC Address**.
- A confirmation warning appears.
- Step 6** Click **Yes**.
- The address disappears from the table of dynamic and static secure MAC addresses.
- Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring a Maximum Number of MAC Addresses

You can configure the maximum number of MAC addresses that can be learned or statically configured on a Layer 2 interface. You can also configure a maximum number of MAC addresses per VLAN on a Layer 2 interface. The largest maximum number of addresses that you can configure is 4096 addresses.



### Note

When you specify a maximum number of addresses that is less than the number of addresses already learned or statically configured on the interface, the device rejects the command. To reduce the number of addresses learned by the sticky or static methods, see the [“Removing a Static Secure MAC Address on an Interface”](#) section on page 10-12.

---

### BEFORE YOU BEGIN

By default, an interface has a maximum of one secure MAC address. VLANs have no default maximum number of secure MAC addresses.

Ensure that port security is enabled. To enable port security, see the [“Enabling or Disabling Port Security Globally”](#) section on page 10-8.

### DETAILED STEPS

To configure the maximum number of secure MAC addresses on an interface, follow these steps:

---

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.
- The available devices appear in the Summary pane.
- Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface on which you want to configure the maximum number of secure MAC addresses.
- The Summary pane displays the slots on the device and any interfaces on which port security is configured. The slot remains selected.
- Step 3** Click the interface on which you want to configure the maximum number of secure MAC addresses.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

- Step 4** From the Details pane, click the **Secure Interface Details** tab.
  - Step 5** (Optional) If you want to configure the maximum number of secure MAC addresses for the interface, expand the **Secure Interface Configuration** section, if necessary, and then enter the new maximum number in the Maximum number of addresses field.
  - Step 6** (Optional) If you want to configure the maximum number of secure MAC addresses for a VLAN on the interface, expand the **Secure Address Configuration** section, if necessary. In the Maximum Number of Secure Addresses column, double-click the entry for the VLAN, and enter the new maximum number.
  - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring an Address Aging Type and Time

You can configure the MAC address aging type and the length of time that the device uses to determine when MAC addresses learned by the dynamic method have reached their age limit.

### BEFORE YOU BEGIN

By default, the aging time is 0 minutes, which disables aging.

Absolute aging is the default aging type.

Ensure that port security is enabled. To enable port security, see the [“Enabling or Disabling Port Security Globally” section on page 10-8](#).

### DETAILED STEPS

To configure address aging for secure MAC addresses on an interface, follow these steps:

- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface on which you want to configure secure MAC address aging.  
The Summary pane displays the slots on the device and any interfaces on which port security is configured. The slot remains selected.
  - Step 3** Click the interface on which you want to configure secure MAC address aging.
  - Step 4** From the Details pane, click the **Dynamic MAC Addresses** tab.
  - Step 5** From the Aging Type drop-down list, pick the aging type.
  - Step 6** In the Age field, enter the number of minutes for the aging period.
  - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring a Security Violation Action

You can configure the action that the device takes if a security violation occurs. The violation action is configurable on each interface that you enable with port security.

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## BEFORE YOU BEGIN

The default security action is to shut down the port on which the security violation occurs.

Ensure that port security is enabled. To enable port security, see the [“Enabling or Disabling Port Security Globally”](#) section on page 10-8.

## DETAILED STEPS

To configure the security violation action on an interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device and then double-click the slot that contains the interface on which you want to configure the security violation action.  
The Summary pane displays the slots on the device and any interfaces on which port security is configured. The slot remains selected.
  - Step 3** Click the interface on which you want to configure the security violation action.
  - Step 4** From the Details pane, click the **Secure Interface Details** tab and then expand the **Secure Interface Configuration** section, if necessary.
  - Step 5** In the Interface Setting area, from the Violation Action drop-down list, choose the security violation action.
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Displaying Secure MAC Addresses

To display secure MAC addresses for an interface, follow these steps:

- 
- Step 1** From the Feature Selector pane, choose **Switching > Layer 2 Security > Port Security**.  
The available devices appear in the Summary pane.
  - Step 2** From the Summary pane, double-click the device
  - Step 3** Double-click the slot that has the interface.
  - Step 4** Click the interface.  
The Secure Interface Details tab and the Dynamic MAC Addresses tab appear in the Details pane.
  - Step 5** (Optional) To display dynamic secure MAC addresses, click the **Dynamic MAC Addresses** tab.  
The Dynamic MAC Addresses tab displays the Host MAC Address table, which lists the dynamic secure MAC addresses per VLAN.
  - Step 6** (Optional) To display static secure MAC addresses, click the **Secure Interface Details** tab and then expand the **Secure Address Configuration** section, if necessary.  
The Secure Address Configuration section displays the Host MAC Address table, which lists the static secure MAC addresses per VLAN.
-

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

## Displaying Violation Statistics

The following window appears in the Violation Statistics tab:

- Port Security Statistics—Displays a chart of security violations for the selected interface.

See the *Cisco DCNM Fundamentals Configuration Guide, Release 4.0* for more information on collecting statistics for this feature.

## Field Descriptions for Port Security

This section includes the following topics:

- [Device: Global Settings Tab, page 10-167](#)
- [Interface: Secure Interface Details: Secure Interface Configuration Section, page 10-16](#)
- [Interface: Secure Interface Details: Secure Address Configuration Section, page 10-17](#)
- [Interface: Dynamic MAC Addresses Tab, page 10-17](#)

### Device: Global Settings Tab

**Table 10-1**      *Device: Global Settings Tab*

Field	Description
Enable Port Security service	Link that enables the port security feature globally on the device. This link appears only when port security is not enabled on the selected device. By default, port security is not enabled.
Stop learning	Whether dynamic secure MAC address learning is globally permitted on the device. By default, this check box is unchecked.

### Interface: Secure Interface Details: Secure Interface Configuration Section

**Table 10-2**      *Interface: Secure Interface Details: Secure Interface Configuration Section*

Field	Description
Interface	<i>Display only.</i> Name of the interface.
Allowed VLANs	<i>Display only.</i> VLANs that packets using the interface can belong to.
Port Type	<i>Display only.</i> Port mode of the interface. Possible values are as follows: <ul style="list-style-type: none"> <li>• Access</li> <li>• Trunk</li> <li>• PVLAN Host</li> <li>• PVLAN Promiscuous</li> </ul> <p><b>Note</b> Port security does not support interfaces in Routed port mode.</p>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

**Table 10-2**      **Interface: Secure Interface Details: Secure Interface Configuration Section (continued)**

Field	Description
Violation Action	Action that the device takes when it detects a security violation on the interface. You can choose one of the following settings: <ul style="list-style-type: none"> <li>• Protect</li> <li>• Restrict</li> <li>• Shutdown (Default)</li> </ul> For more information about violation actions, see the <a href="#">“Security Violations and Actions” section on page 10-4</a> .
Maximum number of addresses	Number of secure MAC addresses allowed on the interface. The default is one secure MAC address.
Number of configured MAC addresses	<i>Display only.</i> Number of static secure MAC addresses configured for the interface.
Number of learnt MAC addresses	<i>Display only.</i> Number of dynamic secure MAC addresses learned for the interface.

## Interface: Secure Interface Details: Secure Address Configuration Section

**Table 10-3**      **Interface: Secure Interface Details: Secure Address Configuration Section**

Field	Description
Host MAC Address	Static secure MAC address. Valid entries are dotted hexadecimal MAC addresses. By default, there are no static secure MAC addresses.

## Interface: Dynamic MAC Addresses Tab

**Table 10-4**      **Interface: Dynamic MAC Addresses Tab**

Field	Description
Port	<i>Display only.</i> Interface name.
Port Type	<i>Display only.</i> Port mode of the interface. Possible values are as follows: <ul style="list-style-type: none"> <li>• Access</li> <li>• Trunk</li> <li>• PVLAN Host</li> <li>• PVLAN Promiscuous</li> </ul> <b>Note</b> Port security does not support interfaces in Routed port mode.

**[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)**

**Table 10-4** Interface: Dynamic MAC Addresses Tab (continued)

Field	Description
Aging Type	Aging type for dynamically learned, secure MAC addresses. You can choose one of the following settings: <ul style="list-style-type: none"> <li>Absolute—Addresses age based how long ago the device learned the address. This is the default setting.</li> <li>InActivity—Addresses age based on how long ago the device last received traffic from the MAC address on the current interface.</li> </ul>
Age	Aging time, in minutes, for dynamically learned, secure MAC addresses. Valid entries are whole numbers from 1 to 1440.
Dynamic MAC Stickiness	Whether the device stores addresses learned by this method in NVRAM. For more information, see the “Sticky Method” section on page 10-2.
Host MAC Address	<i>Display only.</i> MAC addresses secured by the dynamic or sticky address learning method.

## Additional References

For additional information related to implementing port security, see the following sections:

- [Related Documents, page 10-18](#)
- [Standards, page 10-18](#)
- [MIBs, page 10-19](#)

## Related Documents

Related Topic	Document Title
Layer 2 switching	<i>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***

## MIBs

NX-OS provides read-only SNMP support for port security.

MIBs	MIBs Link
<ul style="list-style-type: none"><li data-bbox="147 388 542 415">• CISCO-PORT-SECURITY-MIB</li></ul>	To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/nx-os/mibs">http://www.cisco.com/nx-os/mibs</a>

***Send document comments to [nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com).***