12
Configuring Port Security

All switches in the Cisco MDS 9000 Family provide port security features that reject intrusion attempts and report these intrusions to the administrator.

Note Port security is supported for Fibre Channel ports and Fibre Channel over Ethernet (FCoE) ports as fc-port-security.

This chapter includes the following sections:

About Port Security

All switches in the Cisco MDS 9000 Family provide port security features that reject intrusion attempts and report these intrusions to the administrator.

Typically, any Fibre Channel device in a SAN can attach to any SAN switch port and access SAN services based on zone membership. Port security features prevent unauthorized access to a switch port in the Cisco MDS 9000 Family in the following ways:

- Login requests from unauthorized Fibre Channel devices (Nx ports) and switches (xE ports) are rejected.

- All intrusion attempts are reported to the SAN administrator through system messages.
- Configuration distribution uses the CFS infrastructure, and is limited to those switches that are CFS capable. Distribution is disabled by default.
- Configuring the port security policy requires the ENTERPRISE_PKG license (see the *Cisco MDS 9000 Family NX-OS Licensing Guide*).

This section includes the following topics:

Port Security Enforcement

To enforce port security, configure the devices and switch port interfaces through which each device or switch is connected, and activate the configuration.

- Use the port world wide name (pWWN) or the node world wide name (nWWN) to specify the Nx port connection for each device.
- Use the switch world wide name (sWWN) to specify the xE port connection for each switch.

Each Nx and xE port can be configured to restrict a single port or a range of ports.

Enforcement of port security policies are done on every activation and when the port tries to come up.

The port security feature uses two databases to accept and implement configuration changes.

- Configuration database—All configuration changes are stored in the configuration database.
- Active database—The database currently enforced by the fabric. The port security feature requires all devices connecting to a switch to be part of the port security active database. The software uses this active database to enforce authorization.

About Auto-Learning

You can instruct the switch to automatically learn (auto-learn) the port security configurations over a specified period. This feature allows any switch in the Cisco MDS 9000 Family to automatically learn about devices and switches that connect to it. Use this feature when you activate the port security feature for the first time as it saves tedious manual configuration for each port. You must configure auto-learning on a per-VSAN basis. If enabled, devices and switches that are allowed to connect to the switch are automatically learned, even if you have not configured any port access.

When auto-learning is enabled, learning happens for the devices or interfaces that were already logged into the switch and the new devices or interfaces that need to be logged in. Learned entries on a port are cleaned up after you shut down that port if auto-learning is still enabled.

Learning does not override the existing configured port security policies. So, for example, if an interface is configured to allow a specific pWWN, then auto-learning will not add a new entry to allow any other pWWN on that interface. All other pWWNs will be blocked even in auto-learning mode.

No entries are learned for a port in the shutdown state.

When you activate the port security feature, auto-learning is also automatically enabled.

Note If you activate port security feature, auto-learning gets enabled by default. You cannot re-activate port security until auto-learning is disabled or deactivate and activate again.

Port Security Activation

By default, the port security feature is not activated in any switch in the Cisco MDS 9000 Family.

By activating the port security feature, the following apply:

- Auto-learning is also automatically enabled, which means:
  - From this point, auto-learning happens for the devices or interfaces that were already logged into the switch and also for the new devices will login in future.
  - You cannot activate the database until you disable auto-learning.
- All the devices that are already logged in are learned and are added to the active database.
- All entries in the configured database are copied to the active database.

After the database is activated, subsequent device login is subject to the activated port bound WWN pairs, excluding the auto-learned entries. You must disable auto-learning before the auto-learned entries become activated.

When you activate the port security feature, auto-learning is also automatically enabled. You can choose to activate the port security feature and disable auto-learning.

Tip If a port is shut down because of a denied login attempt, and you subsequently configure the database to allow that login, the port does not come up automatically. You must explicitly issue a **no shutdown** CLI command to bring that port back online.

Port Security Configuration

The steps to configure port security depend on which features you are using. Auto-learning works differently if you are using CFS distribution.

This section includes the following topics:

Configuring Port Security with Auto-Learning and CFS Distribution

To configure port security, using auto-learning and CFS distribution, follow these steps:

Step 1 Enable port security. See the "Enabling Port Security" section on page 12-294.

Step 2 Enable CFS distribution. See the "Enabling Distribution" section on page 12-306.

Step 3 Activate port security on each VSAN. This turns on auto-learning by default. See the "Activating Port Security" section on page 12-296.

Step 4 Issue a CFS commit to copy this configuration to all switches in the fabric. See the "Committing the Changes" section on page 12-307. At this point, all switches are activated, and auto-learning.

Step 5 Wait until all switches and all hosts are automatically learned.

Step 6 Disable auto-learn on each VSAN. See the"Disabling Auto-learning" section on page 12-301.

Step 7 Issue a CFS commit to copy this configuration to all switches in the fabric. See the "Committing the Changes" section on page 12-307. At this point, the auto-learned entries from every switch are combined into a static active database that is distributed to all switches.

Step 8 Copy the active database to the configure database on each VSAN. See the "Copying the Port Security Database" section on page 12-311.

Step 9 Issue a CFS commit to copy this configuration to all switches in the fabric. See the "Committing the Changes" section on page 12-307. This ensures that the configure database is the same on all switches in the fabric.

Step 10 Copy the running configuration to the startup configuration, using the fabric option. This saves the port security configure database to the startup configuration on all switches in the fabric.

Configuring Port Security with Auto-Learning without CFS

To configure port security using auto-learning without CFS, follow these steps:

Step 1 Enable port security. See the "Enabling Port Security" section on page 12-294.

Step 2 Activate port security on each VSAN. This turns on auto-learning by default. See the "Activating Port Security" section on page 12-296.

Step 3 Wait until all switches and all hosts are automatically learned.

Step 4 Disable auto-learn on each VSAN. See the "Disabling Auto-learning" section on page 12-301.

Step 5 Copy the active database to the configure database on each VSAN. See the "Copying the Port Security Database" section on page 12-311.

Step 6 Copy the running configuration to the startup configuration This saves the port security configure database to the startup configuration.

Step 7 Repeat Step 1 through Step 6 for all switches in the fabric.

Configuring Port Security with Manual Database Configuration

To configure port security and manually configure the port security database, follow these steps:

Step 1 Enable port security. See the "Enabling Port Security" section on page 12-294.

Step 2 Manually configure all port security entries into the configure database on each VSAN. See the "Port Security Manual Configuration" section on page 12-303.

Step 3 Activate port security on each VSAN. This turns on auto-learning by default. See the "Activating Port Security" section on page 12-296.

Step 4 Disable auto-learn on each VSAN. See the "Disabling Auto-learning" section on page 12-301.

Step 5 Copy the running configuration to the startup configuration This saves the port security configure database to the startup configuration.

Step 6 Repeat Step 1 through Step 5 for all switches in the fabric.

Configuring Port Security Using the Configuration Wizard

The Port Security Configuration wizard provides step-by-step procedures for setting up the Port Security Policy for a selected VSAN. The Port Security Configuration wizard also supports the central management through CFS, making it possible to complete the entire configuration at one place.

The wizard automatically conducts few essential operations. For example, if you want central management, the wizard conducts operations to check CFS capability, enable CFS, and issue CFS commit at the proper stages.

To manage security at a particular port, you do not need to run through the wizard to configure the port security policy from the VSAN wide, but you can directly edit accesses on the port itself. This operation can be done through the Port Binding dialog box. If the port's belonging switch has not enabled port security yet, the dialog box enables security first. If the port security is enabled, the dialog box will edit the policy database based on user operations.

Prerequisites

The prerequisites for configuring port security are as follows:

- Port security is enabled on the switch.
- Port security policy should be defined either manually by editing bound devices or switches or ports or by using autolearning.
- Port Security policy is activated.
- Activated and configured databases are synchronized through copy.
- Activated database is copied to be the startup configuration.
- CFS should be enabled on all switches in the VSAN. A CFS master switch is selected to do all configurations. All changes will be distributed to the VSAN through the CFS **commit** command.

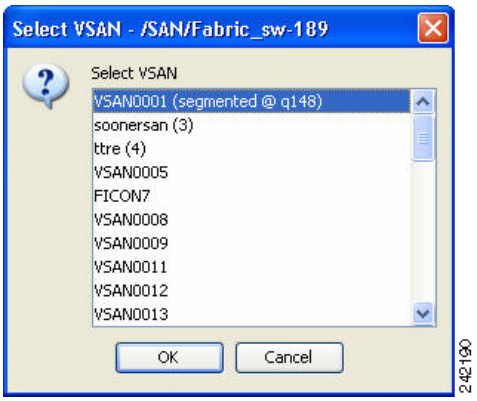
To configure port security, follow these steps:

Step 1 Click the **Port Security**  button on the toolbar.

Before launching the Port Security Setup Wizard, Fabric Manager checks the CFS capability of the switches in the VSAN.

If VSAN context is not available, the wizard prompts to select VSAN as shown in Figure 12-1.

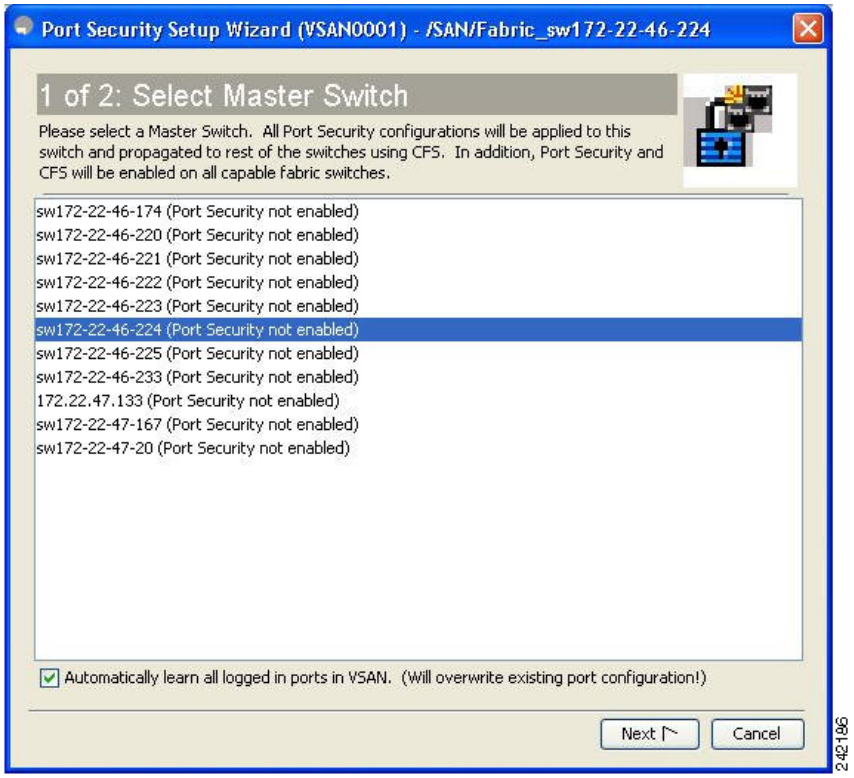
Figure 12-1 Select VSAN Window



Step 2 Select the VSAN from the list and click **OK**.

You see the first page of the **Port Security Setup Wizard** as shown in Figure 12-2.

Figure 12-2 Select Master Switch Page



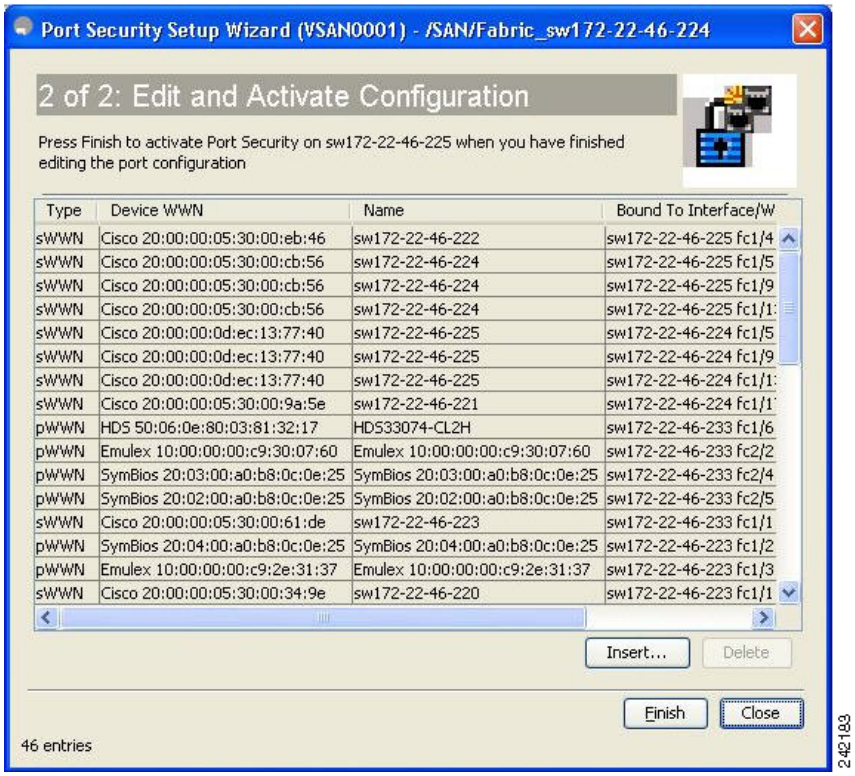
Step 3 Do the following in the **Select Master Switch** page:

- Select the required master switch.
- Select **Automatically learn all logged in ports in VSAN** to Autolearn port configuration.

Step 4 Click **Next** to proceed.

You see **Edit and Activate Configuration** page as shown in Figure 12-3.

Figure 12-3 Edit and Activate Configuration Page



Step 5 Click **Insert** to create port binding.

You see the **Insert Port Security Devices** dialog box as shown in Figure 12-4.

Figure 12-4 Insert Port Security Devices Dialog Box

Step 6 Two types of port binding can be created using the Insert Port Security Devices dialog box:

- **Port WWN**-pWWN bound to an interface WWN.
- **Switch**-Switch WWN bound to an interface. (Mainly useful for ISL binding).

Step 7 Select the type of port binding by clicking the radio buttons and enter the supporting values.

Step 8 Click **OK.**

Step 9 Click **Close** to exit the Insert Port Security window.

Note To delete an entry in the Edit and Activate Configuration page of the wizard, select the entry and click the **Delete** button.

Step 10 Click **Finish** to complete the Port Security Configuration for the selected switch.

Enabling Port Security

By default, the port security feature is disabled in all switches in the Cisco MDS 9000 Family.

To enable port security, follow these steps:

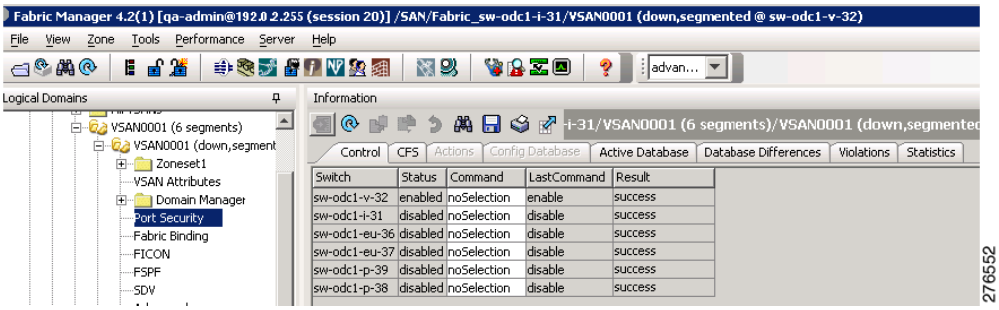
	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# feature port-security`	Enables port security on that switch.
	`switch(config)# no feature port-security`	Disables (default) port security on that switch.

To enable port security using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and then select **Port Securit**y in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane (see Figure 12-5).

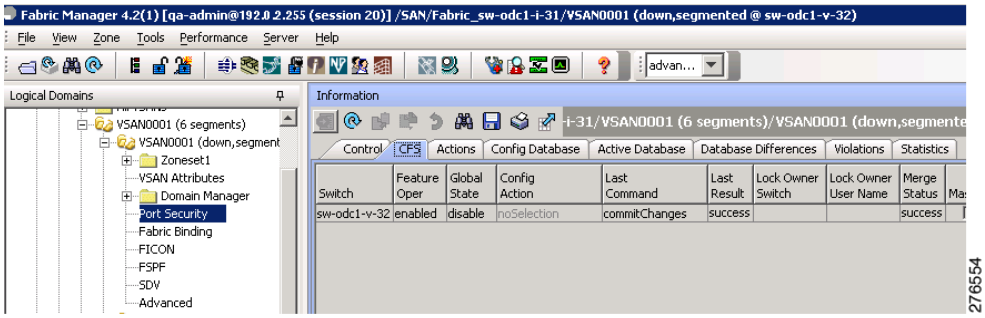
Figure 12-5 Port Security Configuration



Step 2 Click the **CFS** tab.

You see the information show in Figure 12-6.

Figure 12-6 Port Security CFS



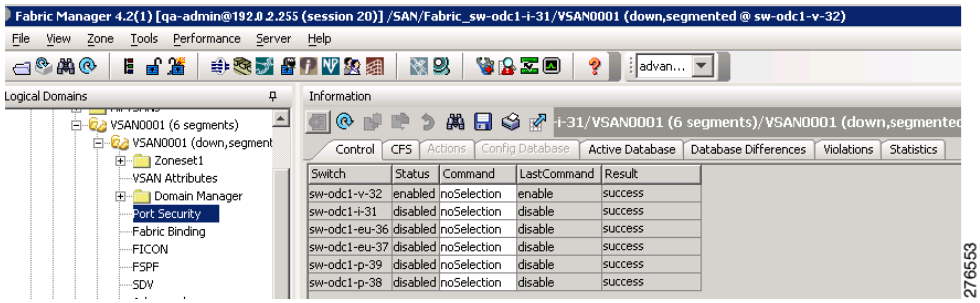
Step 3 Enable CFS on all participating switches in the VSAN by clicking each entry in the Global column and selecting **enable**.

Step 4 Click **Apply Changes** to enable CFS distribution for the port security feature.

Step 5 Click the **Control** tab.

You see the port security enable state for all switches in the selected VSAN (see Figure 12-7).

Figure 12-7 Port Security Configuration



Step 6 Set the Command column to **enable** for each switch in the VSAN.

Step 7 Click the **CFS** tab and set the Command column to **commit** on all participating switches in the VSAN.

Step 8 Click **Apply Changes** to distribute the enabled port security to all switches in the VSAN.

Port Security Activation

This section includes the following topics:

Activating Port Security

To activate the port security feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1`	Activates the port security database for the specified VSAN, and automatically enables auto-learning.
	`switch(config)# port-security activate vsan 1 no-auto-learn`	Activates the port security database for the specified VSAN, and disables auto-learning.
	`switch(config)# no port-security activate vsan 1`	Deactivates the port security database for the specified VSAN, and automatically disables auto-learning.

To activate port security using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Securit**y in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Actions** tab.

Step 3 Click in the Action column under Activation, next to the switch or VSAN on which you want to activate port security. You see a drop-down menu with the following options:

- **activate**—Valid port security settings are activated.
- **activate (TurnLearningOff)**—Valid port security settings are activated and auto-learn turned off.
- **forceActivate**—Activation is forced.
- **forceActivate(TurnLearningOff)**—Activation is forced and auto-learn is turned off.
- **deactivate**—All currently active port security settings are deactivated.
- **NoSelection**— No action is taken.

Step 4 Set the Action field you want for that switch.

Step 5 Uncheck the **AutoLearn** check box for each switch in the VSAN to disable auto-learning.

Step 6 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 7 Click **Apply Changes** in Fabric Manager or **Apply** in Device Manager to save these changes.

Note If required, you can disable auto-learning (see the "Disabling Auto-learning" section on page 12-301).

Database Activation Rejection

Database activation is rejected in the following cases:

- Missing or conflicting entries exist in the configuration database but not in the active database.
- The auto-learning feature was enabled before the activation. To reactivate a database in this state, disable auto-learning.

- The exact security is not configured for each PortChannel member.
- The configured database is empty but the active database is not.

If the database activation is rejected due to one or more conflicts listed in the previous section, you may decide to proceed by forcing the port security activation.

Forcing Port Security Activation

If the port security activation request is rejected, you can force the activation.

Note An activation using the **force** option can log out existing devices if they violate the active database.

You can view missing or conflicting entries using the **port-security database diff active vsan** command in EXEC mode.

To forcefully activate the port security database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security activate vsan 1 force`	Forces the VSAN 1 port security database to activate despite conflicts.

To forcefully activate the port security database using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Securit**y in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Actions** tab.

Step 3 Click in the **Action** column under Activation, next to the switch or VSAN on which you want to activate port security and select the **forceactivate** option.

Step 4 Set the Action field you want for that switch.

Step 5 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 6 Click **Apply Changes** in Fabric Manager or **Apply** in Device Manager to save these changes.

Database Reactivation

To reactivate the port security database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# no port-security auto-learn vsan 1`	Disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learned up to this point.

	Command	Purpose
Step 3	`switch(config)# exit` `switch# port-security database copy vsan 1`	Copies from the active to the configured database.
Step 4	`switch# config t` `switch(config)# port-security activate vsan 1`	Activates the port security database for the specified VSAN, and automatically enables auto-learning.

Tip If auto-learning is enabled, and you cannot activate the database, you will not be allowed to proceed without the **force** option until you disable auto-learning.

To reactivate the port security database using Fabric Manager, follow these steps:

Step 1 Disable auto-learning.

Step 2 Copy the active database to the configured database.

Tip If the active database is empty, you cannot perform this step.

Step 3 Make the required changes to the configuration database.

Step 4 Activate the database.

Copying an Active Database to the Config Database

To copy the active database to the config database using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Securit**y in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Actions** tab.

You see the switches for that VSAN.

Step 3 Check the **CopyActive ToConfig** check box next to the switch for which you want to copy the database.

The active database is copied to the config database when the security setting is activated.

Step 4 Uncheck the **CopyActive ToConfig** check box if you do not want the database copied when the security setting is activated.

Step 5 Click the **CFS** tab and set the command column to **commit** on all participating switches in the VSAN.

Step 6 Click **Apply Changes** to save these changes or click **Undo Changes** to discard any unsaved changes.

Displaying Activated Port Security Settings

To display active port security settings using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Active Database** tab.

You see the active port security settings for that VSAN.

Displaying Port Security Statistics

To display port security statistics using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Statistics** tab.

You see the port security statistics for that VSAN.

Displaying Port Security Violations

Port violations are invalid login attempts (for example, login requests from unauthorized Fibre Channel devices). You can display a list of these attempts on a per-VSAN basis, using Fabric Manager.

To display port security violations, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **Violations** tab. You see the port security violations for that VSAN.

Auto-learning

This section contains the following topics:

About Enabling Auto-learning

The state of the auto-learning configuration depends on the state of the port security feature:

- If the port security feature is not activated, auto-learning is disabled by default.
- If the port security feature is activated, auto-learning is enabled by default (unless you explicitly disabled this option).

Tip If auto-learning is enabled on a VSAN, you can only activate the database for that VSAN by using the **force** option.

Enabling Auto-learning

To enable auto-learning, follow these steps:

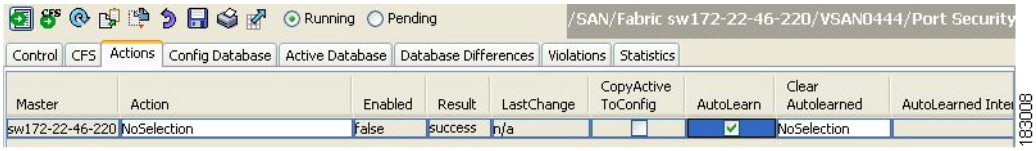
	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security auto-learn vsan 1`	Enables auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database.

To enable auto-learning using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane (see Figure 12-8).

Figure 12-8 Port Security Configuration



Step 2 Click the **Actions** tab.

Step 3 Click in the Action column under Activation, next to the switch or VSAN on which you want to activate port security. You see a drop-down menu with the following options:

- **activate**—Valid port security settings are activated.
- **activate (TurnLearningOff)**—Valid port security settings are activated and auto-learn turned off.
- **forceActivate**—Activation is forced.
- **forceActivate(TurnLearningOff)**—Activation is forced and auto-learn is turned off.
- **deactivate**—All currently active port security settings are deactivated.
- **NoSelection**— No action is taken.

Step 4 Select one of the port security options for that switch.

Step 5 Check the **AutoLearn** check box for each switch in the VSAN to enable auto-learning.

Step 6 Click the **Apply Changes** icon to save these changes.

Disabling Auto-learning

To disable auto-learning, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# no port-security auto-learn vsan 1`	Disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learned up to this point.

To disable auto-learning using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane (see Figure 12-8).

Step 2 Click the **Actions** tab.

You see the switches for that VSAN.

Step 3 Uncheck the **AutoLearn** check box next to the switch if you want to disable auto-learning.

Step 4 Click the **Apply Changes** icon to save these changes.

Auto-learning Device Authorization

Table 12-1 summarizes the authorized connection conditions for device requests.

Table 12-1 Authorized Auto-learning Device Requests

Condition	Device (pWWN, nWWN, sWWN)	Requests Connection to	Authorization
1	Configured with one or more switch ports	A configured switch port	Permitted
2		Any other switch port	Denied
3	Not configured	A switch port that is not configured	Permitted if auto-learning enabled
4			Denied if auto-learning disabled
5	Configured or not configured	A switch port that allows any device	Permitted

Table 12-1 Authorized Auto-learning Device Requests (continued)

Condition	Device (pWWN, nWWN, sWWN)	Requests Connection to	Authorization
6	Configured to log in to any switch port	Any port on the switch	Permitted
7	Not configured	A port configured with some other device	Denied

Authorization Scenarios

Assume that the port security feature is activated and the following conditions are specified in the active database:

- A pWWN (P1) is allowed access through interface fc1/1 (F1).
- A pWWN (P2) is allowed access through interface fc1/1 (F1).
- A nWWN (N1) is allowed access through interface fc1/2 (F2).
- Any WWN is allowed access through interface fc1/3 (F3).
- A nWWN (N3) is allowed access through any interface.
- A pWWN (P3) is allowed access through interface fc1/4 (F4).
- A sWWN (S1) is allowed access through interface fc1/10-13 (F10 to F13).
- A pWWN (P10) is allowed access through interface fc1/11 (F11).

Table 12-2 summarizes the port security authorization results for this active database. The conditions listed refer to the conditions from Table 12-1.

Table 12-2 Authorization Results for Scenario

Device Connection Request	Authorization	Condition	Reason
P1, N2, F1	Permitted	1	No conflict.
P2, N2, F1	Permitted	1	No conflict.
P3, N2, F1	Denied	2	F1 is bound to P1/P2.
P1, N3, F1	Permitted	6	Wildcard match for N3.
P1, N1, F3	Permitted	5	Wildcard match for F3.
P1, N4, F5	Denied	2	P1 is bound to F1.
P5, N1, F5	Denied	2	N1 is only allowed on F2.
P3, N3, F4	Permitted	1	No conflict.
S1, F10	Permitted	1	No conflict.
S2, F11	Denied	7	P10 is bound to F11.
P4, N4, F5 (auto-learning on)	Permitted	3	No conflict.
P4, N4, F5(auto-learning off)	Denied	4	No match.
S3, F5 (auto-learning on)	Permitted	3	No conflict.
S3, F5 (auto-learning off)	Denied	4	No match.
P1, N1, F6 (auto-learning on)	Denied	2	P1 is bound to F1.
P5, N5, F1 (auto-learning on)	Denied	7	Only P1 and P2 bound to F1.

Table 12-2 Authorization Results for Scenario (continued)

Device Connection Request	Authorization	Condition	Reason
S3, F4 (auto-learning on)	Denied	7	P3 paired with F4.
S1, F3 (auto-learning on)	Permitted	5	No conflict.
P5, N3, F3	Permitted	6	Wildcard (*) match for F3 and N3.
P7, N3, F9	Permitted	6	Wildcard (*) match for N3.

Port Security Manual Configuration

To configure port security on any switch in the Cisco MDS 9000 Family, follow these steps:

Step 1 Identify the WWN of the ports that need to be secured.

Step 2 Secure the fWWN to an authorized nWWN or pWWN.

Step 3 Activate the port security database.

Step 4 Verify your configuration.

This section includes the following topics:

About WWN Identification

If you decide to manually configure port security, be sure to adhere to the following guidelines:

- Identify switch ports by the interface or by the fWWN.
- Identify devices by the pWWN or by the nWWN.
- If an Nx port is allowed to log in to SAN switch port Fx, then that Nx port can only log in through the specified Fx port.
- If an Nx port's nWWN is bound to an Fx port WWN, then all pWWNs in the Nx port are implicitly paired with the Fx port.
- TE port checking is done on each VSAN in the allowed VSAN list of the trunk port.
- All PortChannel xE ports must be configured with the same set of WWNs in the same PortChannel.
- E port security is implemented in the port VSAN of the E port. In this case the sWWN is used to secure authorization checks.
- Once activated, the config database can be modified without any effect on the active database.
- By saving the running configuration, you save the configuration database and activated entries in the active database. Learned entries in the active database are not saved.

Adding Authorized Port Pairs

To add authorized port pairs for port security, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security database vsan 1` `switch(config-port-security)#`	Enters the port security database mode for the specified VSAN.
	`switch(config)# no port-security database vsan 1` `switch(config)#`	Deletes the port security configuration database from the specified VSAN.
Step 3	`switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5`	Configures the specified sWWN to only log in through PortChannel 5.
	`switch(config-port-security)# any-wwn interface fc1/1 - fc1/8`	Configures any WWN to log in through the specified interfaces.
	`switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified pWWN to only log in through the specified fWWN.
	`switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e`	Deletes the specified pWWN configured in the previous step.
	`switch(config-port-security)# nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e`	Configures the specified nWWN to log in through the specified fWWN.
	`switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66`	Configures the specified pWWN to log in through any port in the fabric.
	`switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80`	Configures the specified pWWN to log in through any interface in the specified switch.
	`switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80 interface fc3/1`	Configures the specified pWWN to log in through the specified interface in the specified switch
	`switch(config-port-security)# any-wwn interface fc3/1`	Configures any WWN to log in through the specified interface in any switch.
	`switch(config-port-security)# no any-wwn interface fc2/1`	Deletes the wildcard configured in the previous step.

After identifying the WWN pairs that need to be bound, add those pairs to the port security database.

Tip Remote switch binding can be specified at the local switch. To specify the remote interfaces, you can use either the fWWN or sWWN-interface combination.

To add authorized port pairs for port security using Fabric Manager, follow these steps:

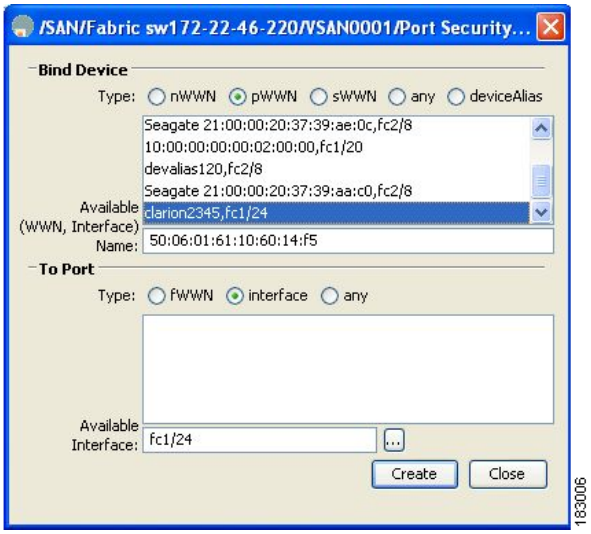
Step 1 Expand a **VSAN** and select **Port Securit**y in the Logical Domains pane.

Step 2 Click the **Config Database** tab.

Step 3 Click **Create Row** to add an authorized port pair.

You see the Create Port Security dialog box shown in Figure 12-9.

Figure 12-9 Create Port Security Dialog Box



Step 4 Double-click the device from the available list for which you want to create the port security setting.

Step 5 Double-click the port from the available list to which you want to bind the device.

Step 6 Click **Create** to create the port security setting.

Step 7 Click the **Apply Changes** icon to save these changes.

Deleting Port Security Setting

To delete a port security setting from the configured database on a switch, follow these steps:

Step 1 Expand a **VSAN** and select **Port Security** in the Logical Domains pane.

Step 2 Click the **Config Database** tab.

You see the configured port security settings for that VSAN.

Step 3 Click the row you want to delete.

Step 4 Click **Delete Row**.

You see the confirmation dialog box.

Step 5 Click **Yes** to delete the row, or click **No** to close the confirmation dialog box without deleting the row.

Step 6 Click the **Apply Changes** icon to save these changes.

Port Security Configuration Distribution

The port security feature uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management, provide a single point of configuration for the entire fabric in the VSAN, and enforce the port security policies throughout the fabric.

This section includes the following topics:

Enabling Distribution

To enable the port security distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security distribute`	Enables distribution.
	`switch(config)# no port-security distribute`	Disables distribution.

For example, if you activate port security, follow up by disabling auto-learning, and commit the changes in the pending database, then the net result of your actions is the same as issuing a **port-security activate vsan** *vsan-id* **no-auto-learn** command.

All the configurations performed in distributed mode are stored in a pending (temporary) database. If you modify the configuration, you need to commit or discard the pending database changes to the configurations. The fabric remains locked during this period. Changes to the pending database are not reflected in the configurations until you commit the changes.

Note Port activation or deactivation and auto-learning enable or disable do not take effect until after a CFS commit if CFS distribution is enabled. Always follow any one of these operations with a CFS commit to ensure proper configuration. See the "Activation and Auto-learning Configuration Distribution" section on page 12-308.

Tip In this case, we recommend that you perform a commit at the end of each operation: after you activate port security and after you enable auto learning.

To enable distribution using Fabric Manager, follow these steps:

Step 1 Expand a **VSAN** and select **Port Securit**y in the Logical Domains pane.

You see the port security configuration for that VSAN in the Information pane (see Figure 12-8).

Step 2 Click the **Control** tab.

You see the switches for that VSAN.

Step 3 In the Command column, select **enable** or **disable** from the drop-down menu.

Step 4 Click the **Apply Changes** icon to save the changes.

Locking the Fabric

The first action that modifies the existing configuration creates the pending database and locks the feature in the VSAN. After you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the pending database.

To display the CFS lock information, use the **show cfs lock** command. For more information, see the *Cisco MDS 9000 Family Command Reference*.

Committing the Changes

If you commit the changes made to the configurations, the configurations in the pending database are distributed to other switches. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

To commit the port security configuration changes for the specified VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security commit vsan 3`	Commits the port security changes in the specified VSAN.

Discarding the Changes

If you discard (abort) the changes made to the pending database, the configuration remains unaffected and the lock is released.

To display the CFS lock information, use the **show cfs lock** command. For more information, see the Cisco MDS 9000 Family Command Reference.

To discard the port security configuration changes for the specified VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# port-security abort vsan 5`	Discards the port security changes in the specified VSAN and clears the pending configuration database.

Activation and Auto-learning Configuration Distribution

Activation and auto-learning configurations in distributed mode are remembered as actions to be performed when you commit the changes in the pending database.

Learned entries are temporary and do not have any role in determining if a login is authorized or not. As such, learned entries do not participate in distribution. When you disable learning and commit the changes in the pending database, the learned entries become static entries in the active database and are distributed to all switches in the fabric. After the commit, the active database on all switches is identical.

If the pending database contains more than one activation and auto-learning configuration when you commit the changes, then the activation and auto-learning changes are consolidated and the behavior may change (see Table 12-3).

Table 12-3 Scenarios for Activation and Auto- learning Configurations in Distributed Mode

Scenario	Actions	Distribution = OFF	Distribution = ON
A and B exist in the configuration database, activation is not done and devices C,D are logged in.	1. You activate the port security database and enable auto-learning.	configuration database = {A,B} active database = {A,B, C[1], D*}	configuration database = {A,B active database = {null} pending database = {A,B + acti be enabled}
	2. A new entry E is added to the configuration database.	configuration database = {A,B, E} active database = {A,B, C*, D*}	configuration database = {A,B active database = {null} pending database = {A,B, E + a to be enabled}
	3. You issue a commit.	Not applicable	configuration database = {A,B, active database = {A,B, E, C*, pending database = empty
A and B exist in the configuration database, activation is not done and devices C,D are logged in.	1. You activate the port security database and enable auto-learning.	configuration database = {A,B} active database = {A,B, C*, D*}	configuration database = {A,B active database = {null} pending database = {A,B + acti be enabled}
	2. You disable learning.	configuration database = {A,B} active database = {A,B, C, D}	configuration database = {A,B active database = {null} pending database = {A,B + acti be enabled + learning to be disabled}
	3. You issue a commit.	Not applicable	configuration database = {A,B active database = {A,B} and de and D are logged out. This is ec activation with auto-learning d pending database = empty

1. The * (asterisk) indicates learned entries.

Tip In this case, we recommend that you perform a commit at the end of each operation: after you activate port security and after you enable auto-learning.

Database Merge Guidelines

A database merge refers to a union of the configuration database and static (unlearned) entries in the active database.

When merging the database between two fabrics, follow these guidelines:

- Verify that the activation status and the auto-learning status is the same in both fabrics.
- Verify that the combined number of configurations for each VSAN in both databases does not exceed 2 K.

Caution If you do not follow these two conditions, the merge will fail. The next distribution will forcefully synchronize the databases and the activation states in the fabric.

Database Interaction

Table 12-4 lists the differences and interaction between the active and configuration databases.

Table 12-4 Active and Configuration Port Security Databases

Active Database	Configuration Database
Read-only.	Read-write.
Saving the configuration only saves the activated entries. Learned entries are not saved.	Saving the configuration saves all the entries in the configuration database.
Once activated, all devices that have already logged into the VSAN are also learned and added to the active database.	Once activated, the configuration database can be modified without any effect on the active database.
You can overwrite the active database with the configured database by activating the port security database. Forcing an activation may violate the entries already configured in the active database.	You can overwrite the configuration database with the active database.

Note You can overwrite the configuration database with the active database using the **port-security database copy vsan** command. The **port-security database diff active vsa**n command in EXEC mode lists the differences between the active database and the configuration database.

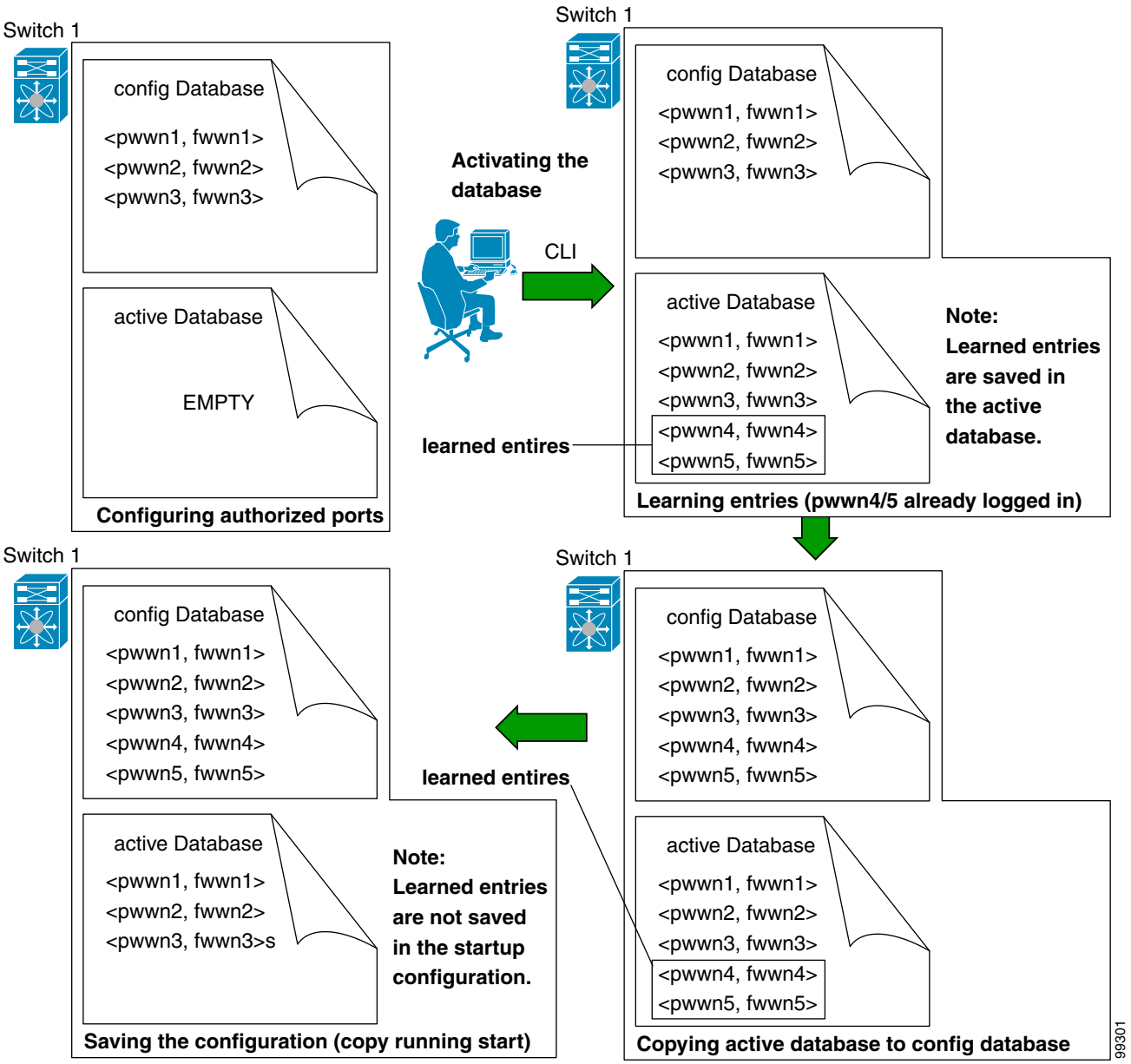
This section includes the following topics:

- Deleting the Port Security Database, page 12-312
- Cleaning the Port Security Database, page 12-312

Database Scenarios

Figure 12-10 depicts various scenarios to depict the active database and the configuration database status based on port security configurations.

Figure 12-10 Port Security Database Scenarios



Copying the Port Security Database

Use the **port-security database copy vsan** command to copy from the active to the configured database. If the active database is empty, this command is not accepted.

```
switch# port-security database copy vsan 1
```

Use the **port-security database diff active vsan** command to view the differences between the active database and the configuration database. This command can be used when resolving conflicts.

```
switch# port-security database diff active vsan 1
```

Use the **port-security database diff config vsan** command to obtain information on the differences between the configuration database and the active database.

```
switch# port-security database diff config vsan 1
```

Tip We recommend that youcopy the active database to the config database issue the **port-security database copy vsan** command after disabling auto-learning. This action will ensure that the configuration database is in sync with the active database. If distribution is enabled, this command creates a temporary copy (and consequently a fabric lock) of the configuration database. If you lock the fabric, you need to commit the changes to the configuration databases in all the switches.

To copy the active database to the configuration database, using Fabric Manager, follow these steps:

Step 1 Expand a **Fabric**, expand a **VSAN** and then select **Port Security** in the Logical Domains pane.

Step 2 Click the **Actions** tab. You see all the configuration databases.

Step 3 Select the appropriate configuration database and check the **Copy Active to Config** check box.

Step 4 Click the **Apply Changes** icon to save your changes.

To view the differences between the active database and the configuration database using Fabric Manager, follow these steps:

Step 1 Expand a **Fabric**, expand a **VSAN** and then select **Port Security** in the Logical Domains pane.

You see the Port Security information in the Information pane.

Step 2 Click the **Database Differences** tab. You see all the configuration databases.

Step 3 Select the appropriate configuration database. Select the **Active** or **Config** option to compare the differences between the selected database and the active or configuration database.

Step 4 Click the **Apply Changes** icon to save your changes.

Deleting the Port Security Database

Tip If the distribution is enabled, the deletion creates a copy of the database. An explicit deletion**port-security commit** command is required to actually delete the database.

Use the **no port-security database vsan** command in configuration mode to delete the configured database for a specified VSAN

```
switch(config)# no port-security database vsan 1
```

To delete a port security database using Fabric Manager, follow these steps:

Step 1 Expand a **Fabric**, expand a **VSAN** and then select **Port Security** in the Logical Domains pane.

You see the Port Security information in the Information pane.

Step 2 Click the **Config Database** tab. You see all the configuration databases.

Step 3 Select the appropriate configuration database and click the **Delete Row** button.

Step 4 Click **Yes** if you want to delete the configuration database.

Cleaning the Port Security Database

Use the **clear port-security statistics vsan** command to clear all existing statistics from the port security database for a specified VSAN.

```
switch# clear port-security statistics vsan 1
```

Use the **clear port-security database auto-learn interface** command to clear any learned entries in the active database for a specified interface within a VSAN.

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

Use the **clear port-security database auto-learn vsan** command to clear any learned entries in the active database for the entire VSAN.

```
switch# clear port-security database auto-learn vsan 1
```

Note The **clear port-security database auto-learn** and **clear port-security statistics** commands are only relevant to the local switch and do not acquire locks. Also, learned entries are only local to the switch and do not participate in distribution.

Use the **port-security clear vsan** command to clear the pending session in the VSAN from any switch in the VSAN.

```
switch# clear port-security session vsan 5
```

To clear all existing statistics from the port security database for a specified VSAN using Fabric Manager, follow these steps:

Step 1 Expand a **Fabric**, expand a **VSAN** and then select **Port Security** in the Logical Domains pane.

You see the Port Security information in the Information pane (see Figure 12-8).

Step 2 Click the **Statistics** tab.

You see all the configuration databases.

Step 3 Select the appropriate configuration database and check the **Clear** option.

Step 4 Click the **Apply Changes icon to save your changes.**

To clear any learned entries in the active database for a specified interface within a VSAN using Fabric Manager, follow these steps:

Step 1 Expand a **Fabric**, expand a **VSAN** and then select **Port Security** in the Logical Domains pane.

You see the Port Security information in the Information pane.

Step 2 Select the **Actions** tab. You see all the configuration databases.

Step 3 Select the appropriate configuration database and check the **AutoLearn** option.

Step 4 Click the **Apply Changes** icon to save your changes.

Note You can clear the Statistics and the AutoLearn option only for switches that are local and do not acquire locks. Also, learned entries are only local to the switch and do not participate in distribution.

Displaying Port Security Configuration

The **show port-security database** commands display the configured port security information (see Examples 12-1 to 12-11).

Example 12-1 Displays the Contents of the Port Security Configuration Database

```
switch# show port-security database
--------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point       (Interface)
--------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)
1       50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/12)
2       20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128)
3       20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

You can optionally specify a fWWN and a VSAN, or an interface and a VSAN in the **show port-security** command to view the output of the activated port security (see Example 12-2).

Example 12-2 Displays the Port Security Configuration Database in VSAN 1

```
switch# show port-security database vsan 1
--------------------------------------------------------------------------------
Vsan   Logging-in Entity              Logging-in Point        (Interface)
--------------------------------------------------------------------------------
1                  *                  20:85:00:44:22:00:4a:9e (fc3/5)
```

```
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

Example 12-3 Displays the Activated Database

```
switch# show port-security database active
--------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point     (Interface)         Learnt
--------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)   20:0d:00:05:30:00:95:de(fc1/13)           Yes
1       50:06:04:82:bc:01:c3:84(pwwn)   20:0c:00:05:30:00:95:de(fc1/12)           Yes
2       20:00:00:05:30:00:95:df(swwn)   20:0c:00:05:30:00:95:de(port-channel 128) Yes
3       20:00:00:05:30:00:95:de(swwn)   20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

Example 12-4 Displays the Contents of the Temporary Configuration Database

```
switch# show port-security pending vsan 1
Session Context for VSAN 1
---------------------------
Activation Status: Active
Auto Learn Status: On
Force activate: No
Config db modified: Yes
Activation done: Yes
Session owner: admin(2)
Session database:
--------------------------------------------------------------------------------
VSAN Logging-in Entity Logging-in Point (Interface)
--------------------------------------------------------------------------------
1 20:11:00:33:22:00:2a:4a(pwwn) 20:41:00:05:30:00:4a:1e(fc2/1)
[Total 1 entries]
```

Example 12-5 Displays the Difference Between the Temporary Configuration Database and the Configuration Database

```
switch# show port-security pending-diff vsan 1
Session Diff for VSAN: 1
-------------------------
Database will be activated
Learning will be turned ON
Database Diff:
+pwwn 20:11:00:33:22:00:2a:4a fwwn 20:41:00:05:30:00:4a:1e
```

The access information for each port can be individually displayed. If you specify the fWWN or interface options, all devices that are paired in the active database (at that point) with the given fWWN or the interface are displayed (see Examples 12-6 to 12-8).

Example 12-6 Displays the Wildcard fWWN Port Security in VSAN 1

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

Example 12-7 Displays the Configured fWWN Port Security in VSAN 1

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
```

```
20:00:00:0c:88:00:4a:e2(swwn)
```

Example 12-8 Displays the Interface Port Information in VSAN 2

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

The port security statistics are constantly updated and available at any time (see Example 12-9).

Example 12-9 Displays the Port Security Statistics

```
switch# show port-security statistics
Statistics For VSAN: 1
-----------------------
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0

Total Logins permitted  : 4
Total Logins denied     : 0
Statistics For VSAN: 2
-----------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
...
```

To verify the status of the active database and the auto-learning configuration, use the **show port-security status** command (see Example 12-10).

Example 12-10 Displays the Port Security Status

```
switch# show port-security status
Fabric Distribution Enabled
VSAN 1 :No Active database, learning is disabled, Session Lock Taken
VSAN 2 :No Active database, learning is disabled, Session Lock Taken
...
```

The **show port-security** command displays the previous 100 violations by default (see Example 12-11).

Example 12-11 Displays the Violations in the Port Security Database

```
switch# show port-security violations

-------------------------------------------------------------------------------------------
VSAN    Interface       Logging-in Entity               Last-Time          [Repeat count]
-------------------------------------------------------------------------------------------
1       fc1/13          21:00:00:e0:8b:06:d9:1d(pwwn)   Jul  9 08:32:20 2003    [20]
                        20:00:00:e0:8b:06:d9:1d(nwwn)
1       fc1/12          50:06:04:82:bc:01:c3:84(pwwn)   Jul  9 08:32:20 2003    [1]
                        50:06:04:82:bc:01:c3:84(nwwn)
2       port-channel 1  20:00:00:05:30:00:95:de(swwn)   Jul  9 08:32:40 2003    [1]
```

```
[Total 2 entries]
```

The **show port-security** command issued with the **last** *number* option displays only the specified number of entries that appear first.

Default Settings

Table 12-5 lists the default settings for all port security features in any switch.

Table 12-5 Default Security Settings

Parameters	Default
Auto-learn	Enabled if port security is enabled.
Port security	Disabled
Distribution	Disabled. **Note** Enabling distribution enables it on all VSANs in the switch.