

How to use NET-SNMP –Port Security

DES-3528 Firmware R2.60 add "*PortSecurity-MIB*" as new MIB files, below are the new instruction of this feature.

The Location of Port Security Management OID:

The screenshot displays a tree view of the PORT-SECURITY-MIB. The 'swPortSecMgmt' node is selected and highlighted. The properties panel on the right provides the following details:

Object name	swPortSecMgmt
Object ID	1.3.6.1.4.1.171.12.63.3
Module	PORT-SECURITY-MIB
Base syntax	Object Identifier
Access	Not_Accessible
Status	Mandatory
Parent node	swPortSecMIB
First child	swPortSecMgmtByPort

::: **MIB:** DES-3528_MIB_R2.60_20100723 -> D-Link-Common-Mgmt -> PortSecurity.mib

::: **OID:** 1.3.6.1.4.1.171.12.63

1) swPortSecCtrl

1.1) swPortSecTrapLogState

Object name	swPortSecTrapLogState
Object ID	1.3.6.1.4.1.171.12.63.1.1
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : enabled(1) 2 : disabled(2)
Parent node	swPortSecCtrl
First child	None
Description	When enabled(1), whenever there's a new MAC address that violates the pre-defined port security configuration, traps will be sent out and the relevant information will be logged into the system.

::: CLI Command:

```
# show port_security  
# enable port_security trap_log
```

::: SNMP Command:

```
# snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.1.1  
# snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.1.1.0 i 1  
(1= enabled; 2=disabled)
```

1.2) swPortSecSysMaxLernAddr

Object name	swPortSecSysMaxLernAddr
Object ID	1.3.6.1.4.1.171.12.63.1.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecCtrl
First child	None
Description	Indicates the maximum number of addresses to be authorized by port security on the system. The max entry range is (1..N). The value N means the max number and is determined by the project itself.

::: CLI Command:

```
# show port_security  
# config port_security system max_learning_addr 1000
```

::: SNMP Command:

```
# snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.1.2  
# snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.1.2.0 i 1000  
1000 = the Max number of learning address on this System
```

2) swPortSecMgmt

2.1) By port: swPortSecPortTable

a) swPortSecPortIndex

Object name	swPortSecPortIndex
Object ID	1.3.6.1.4.1.171.12.63.3.1.1.1.1
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Not_Accessible
Status	Current
Parent node	swPortSecPortEntry
First child	None
Description	Indicates the secured port to lock address learning.

::: **MIB:** swPortSecPortIndex

::: **OID:** 1.3.6.1.4.1.171.12.63.3.1.1.1.1

b) swPortSecPortMaxLernAddr

Object name	swPortSecPortMaxLernAddr
Object ID	1.3.6.1.4.1.171.12.63.3.1.1.1.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecPortEntry
First child	None
Description	Indicates the allowable number of addresses to be learned on this port. The max entry range is (0..N). The value N means the max number and is determined by the project itself.

::: **CLI Command:**

show port_security ports **1**

config port_security ports **1** max_learning_addr **50**

::: **SNMP Command:**

snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.2.**1**

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.2.**1** i **50**

1 = port 1;

50 = the Max number of learning address on this port

c) swPortSecPortLockAddrMode

Object name	swPortSecPortLockAddrMode
Object ID	1.3.6.1.4.1.171.12.63.3.1.1.1.3
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : permanent(1) 2 : deleteOnTimeout(2) 3 : deleteOnReset(3)
Parent node	swPortSecPortEntry
First child	None
Description	Indicates the mode of locking address. In deleteOnTimeout(2) mode, the locked addresses can be aged out after the aging timer expires. In this mode, when the locked address is aged out, the number of addresses that can be learned has to be increased by one. In deleteOnReset (3) mode, locked addresses never age out unless the system restarts which will prevent port movement or intrusion.

::: CLI Command:

```
# show port_security ports 1  
# config port_security ports 1 lock_address_mode permanent
```

::: SNMP Command:

```
# snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.3.1  
# snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.3.1 i 1  
1 = port 1;  
1 = permanent ; 2 = deleteOnTimeout ; 3 = deleteOnReset
```

d) swPortSecPortAdmState

Object name	swPortSecPortAdmState
Object ID	1.3.6.1.4.1.171.12.63.3.1.1.1.4
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : enabled(1) 2 : disabled(2)
Parent node	swPortSecPortEntry
First child	None
Description	Indicates the administration state of the locking address.

::: CLI Command:

```
# show port_security ports 1  
# config port_security ports 1 admin_state enable
```

::: SNMP Command:

```
# snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.4.1  
# snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.4.1 i 1  
1 = port 1;  
1 = enabled; 2 = disabled.
```

e) swPortSecPortClearCtrl

Object name	swPortSecPortClearCtrl
Object ID	1.3.6.1.4.1.171.12.63.3.1.1.1.5
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : other(1) 2 : start(2)
Parent node	swPortSecPortEntry
First child	None
Description	Used to clear port security entries by port. Setting this value to 'start' will execute the clear action. Once cleared, the value returns to 'other'.

::: CLI Command:

clear port_security_entry ports **1**

::: SNMP Command:

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.1.1.1.5.**1 i 2**

1 = port 1;

2 = start to clear

2.2) By vlan: swPortSecVLANTable

a) swPortSecVLANID

Object name	swPortSecVLANID
Object ID	1.3.6.1.4.1.171.12.63.3.2.1.1.1
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Not_Accessible
Status	Current
Value list	1 : 1..4094
Parent node	swPortSecVLANEntry
First child	None
Description	Indicates the secured VLAN to lock address learning.

::: **MIB:** swPortSecVLANID

::: **OID:** 1.3.6.1.4.1.171.12.63.3.2.1.1.1

b) swPortSecVLANMaxLernAddr

Object name	swPortSecVLANMaxLernAddr
Object ID	1.3.6.1.4.1.171.12.63.3.2.1.1.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecVLANEntry
First child	None
Description	Indicates allowable number of addresses to be learned on this VLAN. A value of -1 means no-limit. The default value is no-limit. The max entry range is (0..N). The value N means the max number and is determined by the project itself.

::: **CLI Command:**

show port_security

config port_security vlanid **1** max_learning_addr **100**

::: **SNMP Command:**

snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.2.1.1.2.**1**

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.2.1.1.2.**1** i **100**

1 = VID

100 = the Max number of learning address on this vlan. (-1 means no-limit)

c) swPortSecVLANClearCtrl

Object name	swPortSecVLANClearCtrl
Object ID	1.3.6.1.4.1.171.12.63.3.2.1.1.3
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : other(1) 2 : start(2)
Parent node	swPortSecVLANEntry
First child	None
Description	Used to clear port security entries by VLAN. Setting this value to 'start' will execute the clear action. Once cleared, the value returns to 'other'.

::: CLI Command:

```
# clear port_security_entry
```

::: SNMP Command:

```
# snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.2.1.1.3.1 i 2
```

1 = VID

2 = start to clear

2.3) ByVLANOnPort: swPortSecVLANOnPortTable

2.3.1) swPortSecVLANOnPortTable

a) swPortSecVLANOnPortMaxLernAddr

Object name	swPortSecVLANOnPortMaxLernAddr
Object ID	1.3.6.1.4.1.171.12.63.3.3.1.1.1
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecVLANOnPortEntry
First child	None
Description	Indicates allowable number of addresses to be learned on this VLAN from the special port. A value of -1 means no-limit. The default value is no-limit. Only VLANs with limitations will be displayed in this table. The max entry range is (0..N). The value N means the max number and is determined by the project itself.

::: CLI Command:

show port_security ports **5** vlan **VLAN2**

config port_security ports **5** vlan vlanid **1** max_learning_addr **no_limit**

::: SNMP Command:

snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.3.1.1.1

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.3.1.1.1.**5.1** i **-1**

5 = port 5;

1 = VID;

-1 = no limit

b) swPortSecVLANOnPortAddCtrl

Object name	swPortSecVLANOnPortAddCtrl
Object ID	1.3.6.1.4.1.171.12.63.3.3.1.1.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Create
Status	Current
Value list	1 : other(1) 2 : add(2)
Parent node	swPortSecVLANOnPortEntry
First child	None
Description	other (1): When user gets this object, it always returns other(1). add (2): Used to configure the VLAN limit from the special port. If 'add' is selected, swPortSecVLANOnPortMaxLernAddr must be set to a valid value except -1.

::: CLI Command:

config port_security ports **5** vlan vlanid **1** max_learning_addr **30**

::: SNMP Command:

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.3.1.1.1.**5.1** i **30**
1.3.6.1.4.1.171.12.63.3.3.1.1.2.**5.1** i **2**

5 = port 5;

1 = VID;

30 = the Max number of learning address of this VLAN on the specific port

2 = action “add”

2.3.2) swPortSecMgmtByVLANOnPortClearCtrl

a) swPortSecMgmtByVLANOnPortClearPort

Object name	swPortSecMgmtByVLANOnPortClearPort
Object ID	1.3.6.1.4.1.171.12.63.3.3.2.1
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecMgmtByVLANOnPortClearCtrl
First child	None
Description	Indicates the port.

::: MIB: swPortSecMgmtByVLANOnPortClearPort

::: OID: 1.3.6.1.4.1.171.12.63.3.3.2.1

b) swPortSecMgmtByVLANOnPortClearVID

Object name	swPortSecMgmtByVLANOnPortClearVID
Object ID	1.3.6.1.4.1.171.12.63.3.3.2.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Parent node	swPortSecMgmtByVLANOnPortClearCtrl
First child	None
Description	Indicates the VID.

::: **MIB:** swPortSecMgmtByVLANOnPortClearVID

::: **OID:** 1.3.6.1.4.1.171.12.63.3.3.2.2

c) swPortSecMgmtByVLANOnPortClearAction

Object name	swPortSecMgmtByVLANOnPortClearAction
Object ID	1.3.6.1.4.1.171.12.63.3.3.2.3
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : other(1) 2 : start(2)
Parent node	swPortSecMgmtByVLANOnPortClearCtrl
First child	None
Description	other(1): When user gets this object, it always returns other(1). start(2): Used to clear port security entries by VLAN on the special port.

::: **CLI Command:**

clear port_security_entry ports **5** vlanid **1**

::: **SNMP Command:**

snmpset -c private -v 2c 10.90.90.90 1.3.6.1.4.1.171.12.63.3.3.2.1.0 i **5**

1.3.6.1.4.1.171.12.63.3.3.2.2.0 i **1** 1.3.6.1.4.1.171.12.63.3.3.2.3.0 i **2**

5 = port 5;

1 = VID;

2 = start to clear

2.4) swPortSecEntriesTable

Assume that we've implemented the Port Security feature on port 7, and now its been learnt for few entries when show FDB:

```
DES-3528:admin#sh fdb port 7
Command: show fdb port 7

Unicast MAC Address Aging Time = 300
VID  VLAN Name  MAC Address      Port  Type  Status
-----
1    default    00-00-5E-00-01-0C  7    Static Forward
1    default    00-1C-F0-1C-FA-C4  7    Static Forward
1    default    00-1C-F0-1F-81-04  7    Static Forward

Total Entries: 3
```

a) swPortSecMac

Object name	swPortSecMac
Object ID	1.3.6.1.4.1.171.12.63.3.4.1.1
Module	PORT-SECURITY-MIB
Base syntax	Octet String
Composed syntax	MacAddress
Access	Read-Only
Status	Current
Value list	1 : 6..6
Parent node	swPortSecEntriesEntry
First child	None
Description	Specifies a MAC address.

::: **MIB:** swPortSecMac
::: **OID:** 1.3.6.1.4.1.171.12.63.3.4.1.1

```
C:\>snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.4.1.1
SNMPv2-SMI::enterprises.171.12.63.3.4.1.1.0.94.0.1.12.1 = Hex-STRING: 00 00 5E 00 01 0C
SNMPv2-SMI::enterprises.171.12.63.3.4.1.1.0.28.240.28.250.196.1 = Hex-STRING: 00 1C F0 1C FA C4
SNMPv2-SMI::enterprises.171.12.63.3.4.1.1.0.28.240.31.129.4.1 = Hex-STRING: 00 1C F0 1F 81 04
```

b) swPortSecVID

Object name	swPortSecVID
Object ID	1.3.6.1.4.1.171.12.63.3.4.1.2
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Only
Status	Current
Value list	1 : 1..4094
Parent node	swPortSecEntriesEntry
First child	None
Description	Indicates the VLAN ID.

::: **MIB:** swPortSecVID

::: **OID:** 1.3.6.1.4.1.171.12.63.3.4.1.2

```
C:\>snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.4.1.2
SNMPv2-SMI::enterprises.171.12.63.3.4.1.2.0.0.94.0.1.12.1 = INTEGER: 1
SNMPv2-SMI::enterprises.171.12.63.3.4.1.2.0.28.240.28.250.196.1 = INTEGER: 1
SNMPv2-SMI::enterprises.171.12.63.3.4.1.2.0.28.240.31.129.4.1 = INTEGER: 1
```

c) swPortSecPort

Object name	swPortSecPort
Object ID	1.3.6.1.4.1.171.12.63.3.4.1.3
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Only
Status	Current
Parent node	swPortSecEntriesEntry
First child	None
Description	Indicates the port.

::: **MIB:** swPortSecPort

::: **OID:** 1.3.6.1.4.1.171.12.63.3.4.1.3

```
C:\>snmpwalk -v2c -c private 10.90.90.90 1.3.6.1.4.1.171.12.63.3.4.1.3
SNMPv2-SMI::enterprises.171.12.63.3.4.1.3.0.0.94.0.1.12.1 = INTEGER: 7
SNMPv2-SMI::enterprises.171.12.63.3.4.1.3.0.28.240.28.250.196.1 = INTEGER: 7
SNMPv2-SMI::enterprises.171.12.63.3.4.1.3.0.28.240.31.129.4.1 = INTEGER: 7
```

d) swPortSecDelCtrl

Object name	swPortSecDelCtrl
Object ID	1.3.6.1.4.1.171.12.63.3.4.1.4
Module	PORT-SECURITY-MIB
Base syntax	Integer
Composed syntax	INTEGER
Access	Read-Write
Status	Current
Value list	1 : other(1) 2 : start(2)
Parent node	swPortSecEntriesEntry
First child	None
Description	Used to delete this port security entry. Setting this value to 'start' will execute the delete action. Once deleted, the value returns to 'other'.

::: CLI Command:

```
# delete port_security_entry vlanid 1 mac_address 00-1C-F0-1C-FA-C4
```

::: SNMP Command:

```
# snmpset -c private -v 2c 10.90.90.90  
1.3.6.1.4.1.171.12.63.3.4.1.4.0.28.240.28.250.196.1 i 2  
1 = vlanid;  
00-1C-F0-1C-FA-C4 = 0.28.240.28.250.196 = the MAC you want to delete.  
2 = the action "start"
```