



S Commands

This chapter describes the Cisco NX-OS system management commands that begin with the letter S, excluding the **show** commands.

sampler

To define a sampler and enter the sampler configuration mode, use the **sampler** global configuration mode command. To remove the sampler definition, use the **no** form of this command.

sampler *name*

no sampler *name*

Syntax Description	<i>name</i>	Name of the sampler.
---------------------------	-------------	----------------------

Command Default	No samplers are defined.
------------------------	--------------------------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	NetFlow sampling means that M out of N packets are sampled. When a packet is sampled and there is a NetFlow cache miss, a NetFlow cache entry is created for this flow. The first packet timestamp is updated and the statistics for the first packet are initialized (for example, the bytes are set to the number of bytes
-------------------------	--

Send document comments to nexus7k-docfeedback@cisco.com

in the packet and packet count is set to one). If there is a NetFlow cache hit when the packet is sampled, then the cache for this flow is updated. This includes adding the number of bytes in the packet to the byte counter and incrementing the packet count by one.

Once you enter the **sampler name** command, you enter the sampler configuration mode, and the prompt changes to the following:

```
switch(config-flow-sampler)#
```

Within the sampler configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **description** *description*—Provides a description for this sampler; maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **mode** *sample-num out-of packets*—Configures the sampler mode. The valid values are as follows:
 - *sample-num*—Number of samples per sampling. Range: 1 to 64.
 - **out-of**—Specifies the samples per packet ratio.
 - *packets*—Number of packets in each sampling. Range: 1 to 8192.
- **no**—Negates a command or sets its defaults.

This command does not require a license.

Examples

This example shows how to define a sampler and enter the sampler configuration mode:

```
switch(config)# sampler testsampler
switch(config-flow-sampler)#
```

This example shows how to configure the sampler mode:

```
switch(config)# sampler testsampler
switch(config-flow-sampler)# mode 24 out-of 1200
```

This example shows how to remove a sampler definition:

```
switch(config)# no sampler testsampler
switch(config-flow)#
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow record	Creates a flow record.

Send document comments to nexus7k-docfeedback@cisco.com

save

To save the current configuration session to a file, use the **save** command.

save *location*

Syntax Description	<i>location</i>	Location of the file. The location can be in bootflash:, slot0:, or volatile: The file name can be any alphanumeric string up to 63 characters.
---------------------------	-----------------	---

Defaults	None
-----------------	------

Command Modes	Any
----------------------	-----

Supported User Roles	network-admin vdc-admin
-----------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license.
-------------------------	--

Examples This example shows how to save a configuration session to a file in bootflash:

```
switch# configure session myACLs
switch(config-s)# save bootflash:sessions/myACLs
```

Related Commands	Command	Description
	delete	Deletes a file from a location.

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

scheduler

To schedule a maintenance job, use the **scheduler** command. To disable a job, use the no form of the command. Before using this command to configure a maintenance job, remote users must authenticate with the device using the **scheduler aaa-authentication** command.

```
scheduler {aaa-authentication [username username] password [0 | 7] password |  
job name job-name | logfile size filesize | schedule name schedule-name}
```

```
no scheduler {aaa-authentication [username username] password [0 | 7] password |  
job name job-name | logfile size filesize | schedule name schedule-name}
```

Syntax Description		
aaa-authentication		Begins an AAA authentication exchange with a remote user.
password		Indicates the remote user is entering a password for authentication.
0		Indicates the password is in clear text.
7		Indicates the password is encrypted.
<i>password</i>		The remote user's password.
username <i>username</i>		Indicates the remote user is entering a username, and specifies the username.
logfile		Specifies a logfile configuration.
size <i>filesize</i>		Specifies the size of the logfile. The range is 16 to 1024 KB.
schedule		Defines a schedule for a job.
name <i>schedule-name</i>		Specifies the name of the schedule. The maximum length of the name is 31 characters.
job name <i>job-name</i>		Places you into Job Configuration mode for the specified job name. The maximum length of the name is 31 characters.
LINE		Specify the job configurations separated by semicolons.
end		Returns you to EXEC mode.
exit		Returns you to Global Configuration mode.

Defaults None

Command Modes Configuration mode
Job Configuration mode

SupportedUserRoles Superuser
VDC administrator

Send document comments to nexus7k-docfeedback@cisco.com

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines

To use this command, the scheduler must already be enabled.
 To enable the scheduler, use the **feature scheduler** command.
 This command does not require a license.

**Note**

The commands within a scheduler job must be entered in a single line separated by semicolons (;).

Examples

The following example shows how to schedule a job.

```
switch(config)# scheduler job name test-1
switch(config-job)# conf t;cdp timer 120;snmp community public rw
switch(config-job)# end
switch#
```

The following example shows how to specify the password for a remote user.

```
switch# config t
switch(config)# scheduler aaa-authentication password newpwd
```

The following example shows how to specify a clear text password for a remote user.

```
switch# config t
switch(config)# scheduler aaa-authentication password 0 newpwd
```

The following example shows how to specify an encrypted password for a remote user.

```
switch# config t
switch(config)# scheduler aaa-authentication password 7 newpwd2
```

The following example shows how to specify a name and authentication password for a remote user.

```
switch# config t
switch(config)# scheduler aaa-authentication username admin1 password newpwd3
```

Related Commands

Command	Description
feature scheduler	Enables the scheduler.
show scheduler	Displays scheduler information.

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

snmp-server community

To configure the Simple Network Management Protocol (SNMP) community string, use the **snmp-server community** command. To remove the community string, use the **no** form of this command.

```
snmp-server community name [group name | ro | rw]
```

```
no snmp-server community name [group name | ro | rw]
```

Syntax Description

<i>name</i>	SNMP community string. The name can be any alphanumeric string up to 32 characters.
group name	(Optional) Specifies the group name to which the community belongs. The name can be any alphanumeric string up to 32 characters.
ro	(Optional) Sets read-only access for this community.
rw	(Optional) Sets read-write access for this community.

Defaults

The default community access is read-only (**ro**).

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **snmp-server community** command to configure read-only or read-write access to the SNMP agent on the device. You can optionally configure the community for an access group or user role. See the *Cisco NX-OS Security Configuration Guide, Release 4.0(1)* for more information on user roles.

This command does not require a license.

Examples

This example shows how to configure a read-only SNMP community:

```
switch# configure terminal
switch(config)# snmp-server community test ro
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show snmp community	Displays information about SNMP communities.
show snmp group	Displays information about configured user roles.

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

snmp-server aaa-user cache-timeout

To configure the Simple Network Management Protocol (SNMP) time-out value for synchronized AAA users, use the **snmp-server aaa-user cache-timeout** command. To revert to default, use the **no** form of this command.

```
snmp-server aaa-user cache-timeout seconds
```

```
no snmp-server aaa-user cache-timeout seconds
```

Syntax Description	<i>seconds</i>	Timeout value, in seconds. The range is from 1 to 86400.
Defaults	3600 seconds.	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(3)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to configure the AAA user synchronization timeout value: switch# configure terminal switch(config)# snmp-server aaa-user cache-timeout 6000	
Related Commands	Command	Description
	show snmp	Displays information about SNMP.

Send document comments to nexus7k-docfeedback@cisco.com

snmp-server contact

To configure the Simple Network Management Protocol (SNMP) contact information, use the **snmp-server contact** command. To remove the contact information, use the **no** form of this command.

snmp-server contact [*contact-info*]

no snmp-server contact [*contact-info*]

Syntax Description	<i>contact-info</i> (Optional) SNMP contact information (sysContact). The name can be any alphanumeric string up to 255 characters.
---------------------------	---

Defaults	A zero-length string.
-----------------	-----------------------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	Use the snmp-server contact command to configure the SNMP sysContact variable. This command does not require a license.
-------------------------	---

Examples	This example shows how to configure the SNMP contact: <pre>switch# configure terminal switch(config)# snmp-server contact Jane Smith@anyplace.com</pre>
-----------------	--

Related Commands	Command	Description
	show snmp	Displays information about SNMP.

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

snmp-server context

To configure the Simple Network Management Protocol (SNMP) context to logical network entity mapping, use the **snmp-server context** command. To remove the context, use the **no** form of this command.

snmp-server context *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]

no snmp-server context *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]

Syntax Description

<i>context-name</i>	SNMP context. The name can be any alphanumeric string up to 32 characters.
instance <i>instance-name</i>	(Optional) Specifies a protocol instance. The name can be any alphanumeric string up to 32 characters.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) instance. The name can be any alphanumeric string up to 32 characters.
topology <i>topology-name</i>	(Optional) Specifies the topology. The name can be any alphanumeric string up to 32 characters.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(2)	This command was introduced.

Usage Guidelines

Use the **snmp-server context** command to map between SNMP contexts and logical network entities, such as protocol instances or VRFs.

Do not use the **instance**, **vrf**, or **topology** keywords to delete a context. If you use these keywords, you map the context to a zero-length string.

If you are using SNMPv2c, use the **snmp-server mib community-map** command to map an SNMPv2c community to an SNMP context and use the **snmp-server context** command to map this context to a logical network entity.

See the *Cisco NX-OS Security Configuration Guide* for more information on context mapping.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to map the public1 context to VRF red:

```
switch# configure terminal  
switch(config)# snmp-server context public1 vrf red
```

Related Commands

Command	Description
show snmp context	Displays information about SNMP contexts.
snmp-server mib community-map	Maps an SNMPv2c community to an SNMP context.

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

snmp-server enable traps

To enable the Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps** command. To disable SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps [aaa [server-state-change] | bgp | bridge [topologychange] [newroot]
| callhome | eigrp | entity [fru] | license | link | ospf instance-tag [lsa | rate-limit rate] |
port-security | snmp [authentication] | stp [inconsistency] [loop-consistency]
[root-inconsistency]]
```

```
no snmp-server enable traps [aaa [server-state-change] | bgp | bridge [topologychange]
[newroot] | callhome | eigrp | entity [fru] | license | link | ospf instance-tag [lsa | rate-limit
rate] | port-security | snmp [authentication] | stp [inconsistency] [loop-consistency]
[root-inconsistency]]
```

Syntax Description

aaa	(Optional) Enables AAA notifications.
server-state-change	(Optional) Enables the server-state-change AAA notification.
bgp	(Optional) Enable BGP notifications.
bridge	(Optional) Enable STP Bridge MIB notifications.
topologychange	(Optional) Enable STP topology change notifications.
newroot	(Optional) Enable STP new root bridge notifications.
callhome	(Optional) Enable Call Home notifications.
eigrp	(Optional) Enable EIGRP4-MIB notifications.
entity	(Optional) Enable ENTITY-MIB notifications.
fru	(Optional) Enable ENTITY-FRU-MIB notifications.
license	(Optional) Enable license notifications.
link	(Optional) Enable IF-MIB link notifications.
ospf instance-tag	(Optional) Enable Open Shortest Path First (OSPF) notifications.
lsa	(Optional) Enable OSPF LSA notifications.
rate-limit rate	(Optional) Enable rate limits on OSPF notifications. The range is from 2 to 60 seconds. The default is 10 seconds.
port-security	(Optional) Enable port security notifications.
snmp	(Optional) Enable general SNMP notifications.
authentication	(Optional) Enable SNMP authentication notifications.
stp	(Optional) Enable STPX MIB notifications.
inconsistency	(Optional) Enables SNMP STPX MIB InconsistencyUpdate notifications.
loop-inconsistency	(Optional) Enables SNMP STPX MIB (Optional) Enables SNMP STPX MIB InconsistencyUpdate notifications.
root-inconsistency	(Optional) Enables SNMP STPX MIB RootInconsistencyUpdate notifications.

Defaults

License and SNMP authentication notifications are enabled.

Send document comments to nexus7k-docfeedback@cisco.com

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	Added OSPF rate-limit keyword.
	4.0(3)	Added eigrp keyword.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable BGP notifications:

```
switch# configure terminal  
switch(config) snmp-server enable traps bgp
```

Related Commands	Command	Description
	show snmp trap	Displays the enable or disable state of all SNMP notifications.

Send document comments to nexus7k-docfeedback@cisco.com

snmp-server globalEnforcePriv

To globally enforce privacy for all Simple Network Management Protocol (SNMP) users, use the **snmp-server globalEnforcePriv** command in configuration mode. To disable global privacy, use the **no** form of the command.

snmp-server globalEnforcePriv

no snmp-server globalEnforcePriv

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines Use the **snmp-server globalEnforcePriv** command to enforce privacy on all SNMP users. This command does not require a license.

Examples This example shows how to globally enforce privacy for all SNMP contact:

```
switch# configure terminal
switch(config)# snmp-server contact Jane Smith@anyplace.com
```

Related Commands	Command	Description
	show snmp	Displays information about SNMP.

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

snmp-server host

To configure a host receiver for Simple Network Management Protocol (SNMP) notifications, use the **snmp-server host** command. To remove the specified host, use the **no** form of the command.

```
snmp-server host host-address [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port]
```

```
no snmp-server host host-address [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port]
```

Syntax Description

<i>host-address</i>	Specifies the name or IP address of the host (the targeted recipient).
traps	Sends SNMP traps to this host.
informs	Sends SNMP informs to this host.
version	Specifies the version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the priv keyword.
1	SNMPv1 (default). This option is not available with informs.
2c	SNMPv2C.
3	SNMPv3 has three optional keywords (auth , no auth (default), or priv).
auth	Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
noauth	Specifies the noAuthNoPriv security level.
priv	Enables Data Encryption Standard (DES) packet encryption (privacy).
<i>community-string</i>	Sends a password-like community string with the notification operation.
udp-port <i>port</i>	Specifies the port UDP port of the host to use. The range is from 0 to 65535. The default is 162.

Defaults

Sends SNMP traps.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

The following example configures the recipient of an SNMP notification.

```
switch# config terminal  
switch(config)# snmp-server host 10.1.1.1 traps version 2c abcdsfsf udp-port 500
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server host filter_vrf	Sends only notifications on the specified VRF to the host receiver.
snmp-server host use_vrf	Configures Cisco NX-OS to send notifications on the specified VRF to communicate with an SNMP host receiver.

Send document comments to nexus7k-docfeedback@cisco.com

snmp-server location

To configure the device location used by the Simple Network Management Protocol (SNMP), use the **snmp-server location** command. To remove the location, use the **no** form of the command.

snmp-server location [*location*]

no snmp-server location [*location*]

Syntax Description	<i>location</i>	(Optional) Specifies system location. The location can be any alphanumeric string up to 255 characters.
Defaults	None	
Command Modes	Global configuration	
SupportedUserRoles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example shows how to set the SNMP location: switch# config terminal switch(config)# snmp-server location SanJose	
Related Commands	Command	Description
	show snmp	Displays information about SNMP.

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

snmp-server mib community-map

To configure the Simple Network Management Protocol (SNMP) version 2c community to context mapping, use the **snmp-server mib community-map** command. To remove the community to context mapping, use the **no** form of this command.

snmp-server mib community-map *community-string* **context** *context-name*

no snmp-server mib community-map *community-string* **context** *context-name*

Syntax Description	<i>community-string</i>	SNMP community string. The string can be any alphanumeric string up to 32 characters.
	context <i>context-name</i>	Specifies the SNMP context. The name can be any alphanumeric string up to 32 characters.

Defaults None

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(2)	This command was introduced.

Usage Guidelines Use the **snmp-server mib community-map** command to map between SNMPv2c communities and SNMP contexts. Use the **snmp-server context** command to map this context to a logical network entity. See the *Cisco NX-OS Security Configuration Guide, Release 4.0(1)* for more information on context mapping.

This command does not require a license.

Examples This example shows how to map the public community to the public1 context:

```
switch# configure terminal
switch(config)# snmp-server mib community-map public context public1
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show snmp community	Displays information about SNMP communities.
	show snmp context	Displays information about SNMP contexts.
	snmp-server context	Maps an SNMP context to a logical network entity.

Send document comments to nexus7k-docfeedback@cisco.com

snmp-server protocol enable

To enable the Simple Network Management Protocol (SNMP), use the **snmp-server protocol enable** command. To disable the SNMP protocol, use the **no** form of this command.

snmp-server protocol enable

no snmp-server protocol enable

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(3)	This command was introduced.

Usage Guidelines Use the **no snmp protocol enable** command to disable the SNMP protocol and close any TCP or UDP ports associated with the protocol.

This command does not require a license.

Examples This example shows how disable the SNMP protocol:

```
switch# configure terminal
switch(config)# no snmp-server protocol enable
```

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

snmp-server tcp-session

To enable one time authentication for Simple Network Management Protocol (SNMP) over a TCP session, use the **snmp-server tcp-session** command. To disable one time authentication for SNMP over a TCP session, use the **no** form of the command.

snmp-server tcp-session [auth]

no snmp-server tcp-session [auth]

Syntax Description	auth	Enables one time authentication for SNMP over a TCP session.
Command Default	One time authentication for SNMP over a TCP session is enabled.	
Command Modes	Global configuration	
SupportedUserRoles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	This example enables one time authentication for SNMP over a TCP session. switch# config t switch(config)# snmp-server tcp-session auth	
Related Commands	Command	Description
	show snmp	Displays information about SNMP.

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

snmp-server host filter_vrf

To configure an Simple Network Management Protocol (SNMP) host receiver to gather notifications that occur on a specific virtual routing and forwarding (VRF) instance, use the **snmp-server host filter_vrf** command. To remove the VRF filter, use the **no** form of the command.

```
snmp-server host host-address filter_vrf vrf-name [udp-port port]
```

```
no snmp-server host host-address filter_vrf vrf-name [udp-port port]
```

Syntax Description	Parameter	Description
	<i>host-address</i>	Specifies the name or IP address of the host (the targeted recipient).
	<i>vrf-name</i>	Name of the VRF. The name can be any alphanumeric string up to 63 characters.
	udp-port <i>port</i>	Specifies the port UDP port of the host to use. The range is from 0 to 65535. The default is 162.

Defaults None

Command Modes Global configuration

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples The following example configures the host receiver to receive notifications from the red VRF.

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 filter_vrf red
```

Related Commands	Command	Description
	show snmp	Displays SNMP information.
	snmp-server host	Configures an SNMP hose receiver.
	snmp-server host use_vrf	Configures Cisco NX-OS to send notifications on the specified VRF to communicate with an SNMP hose receiver.

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

snmp-server host use_vrf

To configure the device to communicate with an Simple Network Management Protocol (SNMP) host receiver on a specific virtual routing and forwarding (VRF) instance, use the **snmp-server host use** command. To return to default, use the **no** form of the command.

```
snmp-server host host-address use_vrf vrf-name [udp-port port]
```

```
no snmp-server host host-address use_vrf vrf-name [udp-port port]
```

Syntax Description

<i>host-address</i>	Specifies the name or IP address of the host (the targeted recipient).
<i>vrf-name</i>	Name of the VRF. The name can be any alphanumeric string up to 63 characters.
udp-port <i>port</i>	Specifies the port UDP port of the host to use. The range is from 0 to 65535. The default is 162.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example configures Cisco NX-OS to communicate with the host receiver on the blue VRF.

```
switch# config terminal
switch(config)# snmp-server host 10.1.1.1 use_vrf blue
```

Related Commands

Command	Description
show snmp	Displays SNMP information.
snmp-server host	Configures an SNMP hose receiver.
snmp-server host filter_vrf	Sends only notifications on the specified VRF to the host receiver.

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

snmp-server user enforcePriv

To enforce privacy for an Simple Network Management Protocol (SNMP) user, use the **snmp-server user enforcePriv** command. To revert to factory defaults, use the **no** form of the command.

snmp-server user *username* **enforcePriv**

no snmp-server user *username* **enforcePriv**

Syntax Description	<i>username</i>	Name of user. The name can be any case-sensitive alphanumeric string up to 32 characters.
Defaults	None	
Command Modes	Global configuration	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	The following example enforces privacy for the user joe.	
	<pre>switch# config terminal switch(config)# snmp-server user joe enforcePriv</pre>	
Related Commands	Command	Description
	role name	Configures role profiles used as SNMP group names.
	show snmp	Displays SNMP information.
	snmp-server user	Configures SNMP user information.

Send document comments to nexus7k-docfeedback@cisco.com

snmp-server user

To configure the Simple Network Management Protocol (SNMP) user information, use the **snmp-server user** command. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

```
snmp-server user username [group-name] [auth {md5 | sha} password [priv [aes-128] password] [localizedkey] [engineID id]
```

```
no snmp-server user username [group-name] [auth {md5 | sha} password [priv [aes-128] password] [localizedkey] [engineID id]
```

Syntax Description

<i>username</i>	Name of user. The name can be any case-sensitive alphanumeric string up to 32 characters.
<i>group-name</i>	(Optional) Name of group. The name can be any case-sensitive alphanumeric string up to 32 characters.
auth	(Optional) Sets authentication parameters for the user.
md5	Uses MD5 algorithm for authentication.
sha	Uses SHA algorithm for authentication.
<i>password</i>	User password. The password can be any case-sensitive alphanumeric string up to 64 characters. If you configure the localizedkey keyword, the password can be any case-sensitive alphanumeric string up to 130 characters
priv	(Optional) Sets encryption parameters for the user.
aes-128	(Optional) Sets 128-byte AES algorithm for privacy.
engineID <i>id</i>	Configures the SNMP Engine ID for a notification target user. The engineID format is a 12-digit colon-separated decimal number.
localizedkey	Sets passwords in localized key format. If you configure this keyword, the password can be any case-sensitive alphanumeric string up to 130 characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **snmp-server user** command to configure user authentication and privacy settings for SNMP. If you use the **localizedkey** keyword, you cannot port the SNMP user configuration across devices as the user password contains information on the engine ID of the device. If you copy a configuration file into the device, the passwords may not be set correctly if the configuration file was generated at a different device. We recommend that you explicitly configure passwords after copying the configuration into the device.

Send document comments to nexus7k-docfeedback@cisco.com

SNMP Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword.

To assign multiple roles to a user, configure multiple **snmp-server user** *username* *group-name* commands. The *group-name* argument is defined by the **role name** command.

If you are configuring an SNMP notification target user, use the **engineID** keyword to configure the SNMP engine ID for this user.

This command does not require a license.

Examples

This example sets the user authentication information for user jane.

```
switch# config terminal
switch(config)# snmp-server user jane network-admin auth sha abcd1234
```

This example sets multiple roles for user sam.

```
switch# config terminal
switch(config)# snmp-server user sam network-admin
switch(config)# snmp-server user sam testrole
```

This example sets the user authentication and privacy information for user Juan.

```
switch# config terminal
switch(config)# snmp-server user Juan network-admin auth sha abcd1234 priv abcdefgh
```

This example sets the user authentication and SNMP engine ID for a notification target user.

```
switch# config terminal
switch(config)# snmp-server user notifUser network-admin auth sha abcd1234 engineID
00:12:00:00:09:03:00:05:48:00:74:30
```

Related Commands

Command	Description
role name	Configures role profiles used as SNMP group names.
show snmp	Displays SNMP information.
snmp-server host	Configures SNMP server host information.

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

system cores

To configure the destination for the system core, use the **system cores** command. To revert to the default, use the **no** form of this command.

```
system cores {slot0:[path] | tftp:[server][path]}filename
```

```
no system cores
```

Syntax Description

slot0:	Specifies the slot0: external file system.
<i>path/</i>	(Optional) Directory path to the file. The directory names in the path are case sensitive.
tftp:	Specifies a TFTP server.
<i>/server/</i>	Name or IPv4 address of TFTP server. The server name is case sensitive.
<i>filename</i>	Name for the core file. The name is alphanumeric, case sensitive, and has a maximum of 32 characters.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a core file:

```
switch# configure terminal
switch(config)# system cores slot0:core_file
```

This example shows how to disable system core logging:

```
switch# configure terminal
switch(config)# no system cores
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	clear system cores	Clears the core file.
	show system cores	Displays the core filename.