



SNMP Commands on the Virtual Firewall

This module describes the commands necessary to configure Simple Network Management Protocol (SNMP) on the virtual firewall application. For information on how to configure SNMP on the virtual firewall application, refer to the [“Configuring SNMP on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.



Note

The commands described in this module are SanOS (Linux) commands used on the VFW application. Before you can access any of these commands, you must attach from the route processor to the VFW application using the [service firewall attach location](#) command. For more information, see the [“Attaching to the VFW Application”](#) section in *Cisco IOS XR Virtual Firewall Configuration Guide*.

show snmp

To display the Simple Network Management Protocol (SNMP) statistics and configured SNMP information, use the **show snmp** command in EXEC mode.

show snmp [**community** | **engineID** | **group** | **host** | **sessions** | **user**]

Syntax Description	Parameter	Description
	community	(Optional) Displays SNMP community strings.
	engineID	(Optional) Displays the identification of the local SNMP engine and all remote engines that have been configured on the VFW application.
	group	(Optional) Displays the names of groups on the VFW application, the security model, the status of the different views, and the storage type of each group.
	host	(Optional) Displays the configured SNMP notification recipient host, User Datagram Protocol (UDP) port number, user, and security model.
	sessions	(Optional) Displays the IP address of the targets for which traps or informs have been sent.
	user	(Optional) Displays SNMPv3 user information.

Defaults If no keywords are used, the **show snmp** command displays the VFW application contact, VFW application location, packet traffic information, community strings, and user information.

Command Modes EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

By default, this command displays the VFW application contact, VFW application location, packet traffic information, community strings, and user information. You can instruct the VFW application to display specific SNMP information by including the appropriate keyword.

Examples The following example shows sample output from the **show snmp** command:

```
firewall/Admin# show snmp
sys contact: xxx@cisco.com
```

```

sys location: Training_Lab

0 SNMP packets input
    0 Bad SNMP versions
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
39859 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    39859 Trap PDUs

```

Table 4 describes the fields in the **show snmp** command.

Table 4 Field Descriptions for the show snmp Command Output

Field	Description
Sys contact	Contact name for the SNMP system
Sys location	SNMP system location
SNMP packets input	Total number of SNMP packets received by the VFW application
Bad SNMP versions	Number of packets with an invalid SNMP version
Unknown community name	Number of SNMP packets with an unknown community name
Illegal operation for community name supplied	Number of packets requesting an operation not allowed for that community
Encoding errors	Number of SNMP packets that were improperly encoded
Number of requested variables	Number of variables requested by SNMP managers
Number of altered variables	Number of variables altered by SNMP managers
Get-request PDUs	Number of get requests received
Get-next PDUs	Number of get-next requests received
Set-request PDUs	Number of set requests received
SNMP packets output	Total number of SNMP packets sent by the VFW application
Too big errors	Number of SNMP packets that were larger than the maximum packet size
No such name errors	Number of SNMP requests that specified a MIB object that does not exist
Bad values errors	Number of SNMP set requests that specified an invalid value for a MIB object
General errors	Number of SNMP set requests that failed due to some other error, such as a noSuchName error, badValue error, or any of the other specific errors
Community	The SNMP community name for the VFW application

Table 4 Field Descriptions for the show snmp Command Output (continued)

Field	Description
Group/Access	The access rights for the community: read-only
User	String identifying the name of the SNMP user
Auth	Specifies authentication of a packet without encrypting it
Priv	Specifies authentication of a packet with encryption
Group	User role group to which the user belongs

The following example shows sample output from the **show snmp** command with the **community** keyword:

```
firewall/Admin# show snmp community

Community                Group / Access
-----                -
SNMP_Community1         Network-Monitor
```

[Table 5](#) describes the fields in the **show snmp community** command output.

Table 5 Field Descriptions for the show snmp community Command Output

Field	Description
Community	SNMP community name for the VFW application
Group/Access	Access rights for the community: read-only

The following example shows sample output from the **show snmp snmp** command with the **engineID** keyword:

```
firewall/Admin# show snmp engineID

Local SNMP engineID: 80000009032B18C5A02B13
```

[Table 6](#) describes the fields in the **show snmp engineID** command output.

Table 6 Field Descriptions for the show snmp engineID Command Output

Field	Description
Local SNMP engineID	Identification number of the local SNMP engine on the VFW application

The following example shows sample output from the **show snmp** command with the **group** keyword:

```
firewall/Admin# show snmp group

groupname: Network-Monitor
security model: any
security level: noAuthNoPriv
readview: all
writeview:
notifyview:
storage-type: permanent
row status: active
```

Table 7 describes the fields in the **show snmp group** command output.

Table 7 Field Descriptions for the **show snmp group** Command Output

Field	Description
Group name	Name of the SNMP group or collection of users that have a common access policy
Security model	Security model used by the group, either v1, v2c, or v3
Security level	Security level used by the group
Read view	String identifying the read view of the group
Write view	String identifying the write view of the group
Notify view	String identifying the notify view of the group
Storage-type	Indicates whether the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again
Row status	Indicates whether the Row status for the SNMP group is active or inactive

The following example shows sample output from the **show snmp** command with the **host** keyword:

```
firewall/Admin# show snmp host
```

```
Host                Port  Version  Level  Type  SecName
-----
172.29.52.25       162  v2c      noauth inform SNMP_Community1
```

Table 8 describes the fields in the **show snmp host** command output.

Table 8 Field Descriptions for the **show snmp host** Command Output

Field	Description
Host	IP address of target host
Port	UDP port number to which notifications will be sent
Version	Version of SNMP used to send the trap, either v1, v2c, or v3
Level	Method for authentication and privacy
Type	Type of notification configured
SecName	Security name for scanning the target host

The following example shows sample output from the **show snmp** command with the **sessions** keyword:

```
firewall/Admin# show snmp sessions
```

```
Destination: 172.29.52.25
```

Table 9 describes the fields in the **show snmp sessions** command output.

Table 9 Field Descriptions for the **show snmp sessions** Command Output

Field	Description
Destination	IP address of a target for which traps or informs have been sent

The following example shows sample output from the **show snmp** command with the **user** keyword:

```
firewall/Admin# show snmp user
```

User	Auth	Priv	Groups
www	no	no	Network-Monitor
root	no	no	Network-Monitor
admin	no	no	Network-Monitor
user1	md5	des	Network-Monitor
ciscoSupport	no	no	Network-Monitor

Table 10 describes the fields in the **show snmp user** command output.

Table 10 Field Descriptions for the show snmp user Command Output

Field	Description
User	String identifying the name of the SNMP user
Auth	Specifies authentication of a packet without encrypting it
Priv	Specifies authentication of a packet with encryption
Group	User role group to which the user belongs

Related Commands

Command	Description
snmp-server community	Creates or modifies SNMP community names and access privileges.
snmp-server contact	Specifies the contact information for the SNMP system.
snmp-server enable traps	Enables the VFW application to send SNMP traps and informs to the NMS.
snmp-server host	Specifies which host receives SNMP notifications.
snmp-server location	Specifies the SNMP system location.
snmp-server trap link ietf	Instructs the VFW application to send the linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus.
snmp-server user	Configures SNMP user information.

snmp-server community

To create or modify Simple Network Management Protocol (SNMP) community names and access privileges, use the **snmp-server community** command in configuration mode. To remove an SNMP community, use the **no** form of this command.

```
snmp-server community community_string [group group_name | ro]
```

```
no snmp-server community community_name [group group_name | ro]
```

Syntax Description

<i>community_string</i>	SNMP community name for this system. Enter an unquoted text string with no space and a maximum of 32 characters.
group <i>group_name</i>	(Optional) Identifies the role group to which the user belongs. Enter an unquoted text string with no space and a maximum of 32 characters. Note Only network monitoring operations are supported through the VFW application implementation of SNMP. In this case, all SNMP users are automatically assigned the system-defined default group of Network-Monitor. For details on creating users, see the <i>Cisco Virtual Firewall Configuration Guide</i> .
ro	(Optional) Allows read-only access for this community.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **snmp-server community** command to create or modify SNMP community names and access privileges. Each SNMP device or member is part of a community, use the **snmp-server community** command. An SNMP community determines the access rights for each SNMP device. SNMP uses communities to establish trust between managers and agents.

After you create or modify a community, all SNMP devices assigned to that community as members have the same access rights (as described in RFC 2576). The VFW application supports read-only access to the Management Information Base (MIB) tree for devices included in this community. The read-only community string allows a user to read data values, but prevents that user from modifying the data.

SNMP communities are applicable only for SNMPv1 and SNMPv2c. SNMPv3 requires user configuration information such as specifying the role group that the user belongs to, authentication parameters for the user, authentication password, and message encryption parameters.

Examples

The following example shows how to specify an SNMP community called SNMP_Community1, a member of the user group, with read-only access privileges for the community:

```
firewall/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor
```

Related Commands

Command	Description
snmp-server host	Specifies which host receives SNMP notifications.

snmp-server contact

To specify the contact information for the Simple Network Management Protocol (SNMP) system, use the **snmp-server contact** command in configuration mode. To remove an SNMP contact, use the **no** form of this command.

snmp-server contact *contact_information*

no snmp-server contact

Syntax Description

<i>contact_information</i>	SNMP contact information for this system. Enter as a text string with a maximum of 240 characters including spaces. You can include information on how to contact the person; for example, a phone number or an e-mail address.
----------------------------	---

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You can specify only one contact name per SNMP system.

Examples

The following example shows how to specify SNMP system contact information:

```
firewall/Admin(config)# snmp-server contact User1 user1@cisco.com
```

Related Commands

Command	Description
snmp-server host	Specifies which host receives SNMP notifications.

snmp-server enable traps

To enable the VFW application to send Simple Network Management Protocol (SNMP) traps and informs to the Network Management System (NMS), use the **snmp-server enable traps** command in configuration mode. To disable the sending of SNMP traps and inform requests, use the **no** form of this command.

snmp-server enable traps [*notification_type*] [*notification_option*]

no snmp-server enable traps [*notification_type*] [*notification_option*]

Syntax Description

<i>notification_type</i>	(Optional) Type of notification to enable. If no type is specified, the VFW application sends all notifications. Specify one of the following keywords: <ul style="list-style-type: none"> • license—Sends SNMP license manager notifications. This keyword appears only in the Admin context. • slb—Sends server load-balancing notifications. When you specify the slb keyword, you can specify a <i>notification_option</i> value. • snmp—Sends SNMP notifications. When you specify the snmp keyword, you can specify a <i>notification_option</i> value. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command. • virtual-context—Sends virtual context change notifications. This keyword appears only in the Admin context.
<i>notification_option</i>	(Optional) One of the following SNMP notifications to enable: <ul style="list-style-type: none"> • When you specify the snmp keyword, specify the authentication, coldstart, linkdown, or linkup keyword to enable SNMP notifications. This selection generates a notification if the community string provided in the SNMP request is incorrect, or when an interface is either up or down. The coldstart keyword appears only in the Admin context. • When you specify the slb keyword, specify the real or vserver keyword to enable server load-balancing notifications. This selection generates a notification if: <ul style="list-style-type: none"> – The real server changes state (up or down) due to occurrences such as user intervention, ARP failure, and probe failure. – The virtual server changes state (up or down). The virtual server represents the servers behind the content switch in the VFW application to the outside world and consists of the following attributes: destination address (can be a range of IP addresses), protocol, destination port, incoming interface.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **snmp-server enable traps** command to enable the VFW application to send SNMP traps and informs to the NMS. This command enables both traps and inform requests for the specified notification types.

The notification types used in the **snmp-server enable traps** command all have an associated MIB object that globally enables or disables them. However, not all the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of the notification types cannot be controlled using the **snmp-server enable** command.

To configure the VFW application to send the SNMP notifications, specify at least one **snmp-server enable traps** command. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option. If you enter the command without any keywords, the VFW application enables all notification types and traps.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. The **snmp-server host** command specifies which host receives the SNMP notifications. To send notifications, you must configure at least one SNMP server host.

Examples

The following example shows how to enable the VFW application to send server load-balancing traps to the host myhost.cisco.com using the community string public:

```
firewall/Admin(config)# snmp-server host myhost.cisco.com
firewall/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor
firewall/Admin(config)# snmp-server enable traps slb real
```

Related Commands

Command	Description
snmp-server host	Specifies which host receives SNMP notifications.

snmp-server host

To specify which host receives Simple Network Management Protocol (SNMP) notifications, use the **snmp-server host** command in configuration mode. To remove the specified host, use the **no** form of this command.

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

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

Syntax Description

<i>host_address</i>	IP address of the host (the targeted recipient). Enter the address in dotted-decimal IP notation.
<i>community-string</i>	SNMP community string or username with the notification operation to send. Enter an unquoted text string with no space and a maximum of 32 characters.
informs	Sends SNMP inform requests to the identified host, which allows for manager-to-manager communication. The use of inform requests can be useful when the need arises for more than one NMS in the network.
traps	Sends SNMP traps to the identified host. A trap is the method for an agent to tell the NMS that a problem has occurred. The trap originates from the agent and is sent to the trap destination, as configured within the agent itself. The trap destination is typically the IP address of the NMS.
version	Specifies the version of SNMP used to send the traps. SNMPv3 is the most secure model because it allows packet encryption with the priv keyword.
1	Specifies SNMPv1. This keyword is not available for use with SNMP inform requests.
2c	Specifies SNMPv2C.
3	Specifies SNMPv3.
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).
udp-port <i>port_number</i>	Specifies the port UDP port of the host to use. Enter an integer from 0 to 65535. The default is 162.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **snmp-server host** command to specify which host receives SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to specify the recipient of an SNMP notification:

```
firewall/Admin(config)# snmp-server host 192.168.1.1 traps version 2c abcdsfsf udp-port 500
```

Related Commands

Command	Description
snmp-server enable traps	Enables the VFW application to send SNMP traps and informs to the NMS.

snmp-server location

To specify the Simple Network Management Protocol (SNMP) system location, use the **snmp-server location** command in configuration mode. To remove the SNMP system location, use the **no** form of this command.

snmp-server location *location*

no snmp-server location

Syntax Description

<i>location</i>	Physical location of the system. Enter a text string with a maximum of 240 characters including spaces.
-----------------	---

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You can specify only one location per SNMP system.

Examples

The following example shows how to specify SNMP system location information:

```
firewall/Admin(config)# snmp-server location Boxborough MA
```

Related Commands

Command	Description
snmp-server community	Creates or modifies SNMP community names and access privileges.

snmp-server trap link ietf

To instruct the VFW application to send the linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus, use the **snmp-server trap link ietf** command in configuration mode. To revert to the Cisco implementation of linkUp and linkDown traps, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

Usage Guidelines This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

By default, the VFW application sends the Cisco implementation of linkUp and linkDown traps to the NMS. The VFW application sends the Cisco Systems IF-MIB variable bindings, which consists of ifIndex, ifAdminStatus, ifOperStatus, ifName, ifType, clogOriginID, and clogOriginIDType. You can configure the VFW application to send the IETF standards-based implementation for linkUp and linkDown traps (as outlined in RFC 2863).

The Cisco var-binds are sent by default. To receive RFC 2863 compliant traps, you must specify the **snmp-server trap link ietf** command.

Examples The following example shows how to configure the linkUp and linkDown traps to be compliant with RFC 2863:

```
firewall/Admin(config)# snmp-server trap link ietf
```

snmp-server trap link ietf

Related Commands	Command	Description
	snmp-server enable traps	Enables the VFW application to send SNMP traps and informs to the NMS.

snmp-server trap-source interface

To specify the use of the IP address configured on an interface as the trap-source address in the Simple Network Management Protocol version 1 (SNMPv1) trap protocol data unit (PDU), use the **snmp-server trap-source** command in configuration mode. To remove the specified interface as the trap source address in the SNMPv1 trap PDU and reset the default behavior, use the **no** form of this command.

snmp-server trap-source interface

no snmp-server trap-source interface

Defaults

By default, the VFW application uses the trap source IP address from the internal routing table, depending on the destination host address, where the VFW application will send the notification.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **snmp-server trap-source** command to specify the use of the IP address configured on an interface as the trap-source address in the SNMPv1 trap PDU. By default, the VFW application uses the trap source IP address from the internal routing table, depending on the destination host address, where the VFW application will send the notification.

If interface does not have a valid IP address, the sending of notifications fails for SNMPv1 traps.

Examples

The following example shows how to specify interface abc as the interface for the source address in the SNMPv1 trap PDUs:

```
firewall/Admin(config)# snmp-server trap-source interface abc
```

Related Commands

Command	Description
snmp-server enable traps	Enables the VFW application to send SNMP traps and informs to the NMS.

snmp-server user

To configure Simple Network Management Protocol (SNMP) user information, use the **snmp-server user** command in configuration mode. To disable the SNMP user configuration or to remove an SNMP user, use the **no** form of this command.

```
snmp-server user user_name [group_name] [auth {md5 | sha} password1 [localizedkey] [priv
password2 | aes-128 password2]]
```

```
no snmp-server user user_name [group_name] [auth {md5 | sha} password1 [localizedkey] [priv
password2 | aes-128 password2]]
```

Syntax Description

<i>user_name</i>	Username. Enter an unquoted text string with no space and a maximum of 24 characters.
<i>group_name</i>	(Optional) User role group to which the user belongs. Enter an unquoted text string with no space and a maximum of 32 characters. SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. The <i>group_name</i> is defined by the role configuration mode command.
auth	(Optional) Sets authentication parameters for the user. Authentication determines that the message is from a valid source.
md5	Specifies the HMAC Message Digest 5 (MD5) encryption algorithm for user authentication.
sha	Specifies the HMAC Secure Hash Algorithm (SHA) encryption algorithm for user authentication.
<i>password1</i>	User authentication password. Enter an unquoted text string with no space and a maximum of 130 characters. The VFW application automatically synchronizes the SNMP authentication password as the password for the CLI user.
localizedkey	(Optional) Specifies that the password is in localized key format for security encryption.
priv	(Optional) Specifies encryption parameters for the user. The priv keyword, along with aes-128 keyword, indicates that this privacy password is for generating a 128-bit AES key.
aes-128	(Optional) Specifies the 128-byte Advanced Encryption Standard (AES) algorithm for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption. It conforms with RFC 3826.
<i>password2</i>	Encryption password for the user. The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters. If you use the localized key, you can specify a maximum of 130 characters. Spaces are not allowed.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To assign multiple roles to a user, enter multiple **snmp-server user** commands.

User configuration through the **snmp-server user** command is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication.

The VFW application synchronizes the interactions between the user created by the **username** command and by the **snmp-server user** command; updates to a user through the VFW application command-line interface (CLI) are automatically reflected in the SNMP server. For example, deleting a user automatically results in the user being deleted for both SNMP and CLI. In addition, user-role mapping changes are synchronized in SNMP and CLI.

Only network monitoring operations are supported through the VFW application implementation of SNMP. In this case, all SNMP users are automatically assigned the system-defined default group of Network-Monitor.

Examples

The following example shows how to set the user information:

```
firewall/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
firewall/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234
firewall/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcdefgh
firewall/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh
```

The following example shows how to disable the SNMP user configuration or to remove an SNMP user:

```
firewall/Admin(config)# no snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh
```

Related Commands

Command	Description
snmp-server community	Creates or modifies SNMP community names and access privileges.

