

## Chapter 13

# Summary of SNMPv3 Configuration Statements

The following sections explain each of the SNMPv3 configuration statements. The statements are organized alphabetically.

### address

---

<b>Syntax</b>	<code>address <i>address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
<b>Description</b>	Specify the SNMP target address.
<b>Options</b>	<i>address</i> —IPv4 address of the system to receive traps. You must specify an address, not a hostname.
<b>Usage Guidelines</b>	See “Configuring the Address” on page 65.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration

### address-mask

---

<b>Syntax</b>	<code>address-mask <i>address-mask</i>;</code>
<b>Hierarchy Level</b>	<code>[edit snmp v3 target-address <i>target-address-name</i>]</code>
<b>Description</b>	Verify the source addresses for a group of target addresses.
<b>Options</b>	<i>address-mask</i> combined with the address defines a range of addresses.
<b>Usage Guidelines</b>	See “Configuring the Address Mask” on page 66.
<b>Required Privilege Level</b>	<code>snmp</code> —To view this statement in the configuration. <code>snmp-control</code> —To add this statement to the configuration

## authentication-md5

---

**Syntax** authentication-md5 {  
    authentication-password *authentication-password*;  
}

**Hierarchy Level** [edit snmp v3 usm local-engine user *username*]

**Description** Configure the MD5 as the authentication type for the SNMPv3 user.

**Options** *authentication-password*—Password that generates the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a routing platform:

The password must be at least 8 characters long.

You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.



**NOTE:** You can only configure one authentication type for each SNMPv3 user.

---

**Usage Guidelines** See “Configuring the MD5 Authentication” on page 50.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## authentication-none

---

**Syntax** authentication-none;

**Hierarchy Level** [edit snmp v3 usm local-engine user *username*]

**Description** Configure no authentication for the SNMPv3 user.



**NOTE:** You can only configure one authentication type for each SNMPv3 user.

---

**Usage Guidelines** See “Configuring No Authentication” on page 51.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## authentication-password

---

<b>Syntax</b>	<code>authentication-password <i>authentication-password</i>;</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> authentication-md5], [edit snmp v3 usm local-engine user <i>username</i> authentication-sha]
<b>Description</b>	Configure password for authentication.
<b>Options</b>	<i>authentication-password</i> —Password used to generate the key used for authentication.  SNMPv3 has special requirements when you create plain-text passwords on a routing platform:  The password must be at least 8 characters long.  You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.
<b>Usage Guidelines</b>	See “Configuring the MD5 Authentication” on page 50 and “Configuring the SHA Authentication” on page 51.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## authentication-sha

---

<b>Syntax</b>	<code>authentication-sha {     authentication-password <i>authentication-password</i>; }</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ]
<b>Description</b>	Configure the SHA as the authentication type for the SNMPv3 user



**NOTE:** You can only configure one authentication type for each SNMPv3 user.

---

**Options** *authentication-password*—The password used to generate the key used for authentication.

SNMPv3 has special requirements when you create plain-text passwords on a routing platform:

The password must be at least 8 characters long.

You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.

**Usage Guidelines** See “Configuring the SHA Authentication” on page 51.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## community-name

---

**Syntax** community-name *community-name*;

**Hierarchy Level** [edit snmp v3 snmp-community *community-index*]

**Description** The community name defines an SNMP community. The SNMP community authorizes SNMPv1 or SNMPv2 clients. The access privileges associated with the configured security name define which MIB objects are available and the operations (notify, read, or write) allowed on those objects

**Options** *community-name*—A community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose it in quotation marks (" ").



**NOTE:** Community names must be unique. You cannot configure the same community name at the [edit snmp community] and [edit snmp v3 snmp-community *community-index*] hierarchy levels.

The community name at the [edit snmp v3 snmp-community *community-index*] hierarchy level is encrypted and not displayed in the CLI.

---

**Usage Guidelines** See “Configuring the SNMP Community” on page 72.


**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## engine-id

---

<b>Syntax</b>	engine-id { (local <i>engine-id-suffix</i>   use-default-ip-address   use-mac-address); }
<b>Hierarchy Level</b>	[edit snmp]
<b>Description</b>	The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> . You can configure the suffix here.

---

	<b>NOTE:</b> SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords will be based on the previous engine ID.
	For the engine ID, we recommend using the MAC address of fxp0.

---

<b>Options</b>	<p>local <i>engine-id-suffix</i>—The engine ID suffix is explicitly configured.</p> <p>use-default-ip-address—The engine ID suffix is generated from the default IP address.</p> <p>use-mac-address—The SNMP engine identifier is generated from the MAC address of the management interface on the routing platform.</p> <p><b>Default:</b> use-default-ip-address</p>
<b>Usage Guidelines</b>	See “Configuring the Local Engine ID” on page 48.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## group

---

See the following sections:

group (Configuring) on page 152

group (Defining Access Privileges for an SNMPv3 Group) on page 152

### **group (Configuring)**

<b>Syntax</b>	group <i>group-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 vacm access]
<b>Description</b>	Assign the security name to a group.
<b>Options</b>	<i>group-name</i> —SNMPv3 group name created for the SNMPv3 group.
<b>Usage Guidelines</b>	See “Configuring the Group” on page 57.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

### **group (Defining Access Privileges for an SNMPv3 Group)**

<b>Syntax</b>	group <i>group-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 vacm security-to-group security-model (usm   v1   v2) security-name <i>security-name</i> ]
<b>Description</b>	Define access privileges granted to a group.
<b>Options</b>	<i>group-name</i> —Identifies a collection of SNMP security names that belong to the same access policy SNMP.
<b>Usage Guidelines</b>	See “Configuring the Group” on page 61.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## local-engine

```

Syntax local-engine {
    user username {
        authentication-md5 {
            authentication-password authentication-password;
        }
        authentication-sha {
            authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
            privacy-password privacy-password;
        }
        privacy-des {
            privacy-password privacy-password;
        }
        privacy-3des {
            privacy-password privacy-password;
        }
        privacy-none {
            privacy-password privacy-password;
        }
    }
}

```

**Hierarchy Level** [edit snmp v3 usm]

**Description** Configure local-engine information for the user-based security model (USM).

The remaining statements are explained separately.

**Usage Guidelines** See “Creating SNMPv3 Users” on page 49.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## message-processing-model

---

<b>Syntax</b>	message-process-model (v1   v2c   v3);
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameter-name</i> parameters]
<b>Description</b>	Configure the message processing model to be used when generating SNMP notifications.
<b>Options</b>	v1—SNMPv1 message process model. v2c—SNMPv2c message process model. v3—SNMPv3 message process model.
<b>Usage Guidelines</b>	See “Configuring the Message Processing Model” on page 69.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## notify

---

<b>Syntax</b>	notify <i>name</i> { tag <i>tag-name</i> ; type trap; }
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Description</b>	Select management targets for notifications as well as the type of notifications.
<b>Options</b>	<i>name</i> —Name assigned to the notification. <i>tag-name</i> —Notifications that are sent to all targets configured with this tag. type—Notification type is trap.
<b>Usage Guidelines</b>	See “Configuring the Trap Target Address” on page 65.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## notify-filter

---

See the following sections:

notify-filter (Applying to Management Target) on page 155

notify-filter (Configuring) on page 155

### ***notify-filter (Applying to Management Target)***

<b>Syntax</b>	notify-filter <i>profile-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> ]
<b>Description</b>	Specify the notify filter to use by a specific set of target parameters.
<b>Options</b>	<i>profile-name</i> —Name of the notify filter to apply to notifications.
<b>Usage Guidelines</b>	See “Applying the Trap Notification Filter” on page 69.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

### ***notify-filter (Configuring)***

<b>Syntax</b>	notify-filter <i>profile-name</i> { oid <i>oid</i> (include   exclude); }
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Description</b>	Define a group of MIB objects on which to define access. The notify filter limits the type of traps sent to the NMS.
<b>Options</b>	<i>profile-name</i> —Name assigned to the notify filter.  The remaining statement is explained separately.
<b>Usage Guidelines</b>	See “Configuring the Trap Notification Filter” on page 64.
<b>See Also</b>	oid on page 156.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## notify-view

---

<b>Syntax</b>	notify-view <i>view-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 vacm access group <i>group-name</i> default-context-prefix security-model (any   usm   v1   v2c) security-level (authentication   none   privacy)]
<b>Description</b>	Associate the view with a community or a group name (SNMPv3).
<b>Options</b>	<i>view-name</i> —Name of the view to which the SNMP user group has access.
<b>Usage Guidelines</b>	See “Configuring the Notify View” on page 58.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>See Also</b>	See “Configuring MIB Views” on page 54.

## oid

---

<b>Syntax</b>	oid <i>oid</i> (include   exclude);
<b>Hierarchy Level</b>	[edit snmp v3 notify-filter <i>profile-name</i> ]
<b>Description</b>	Specify an object identifier (OID) used to represent a subtree of MIB objects.
<b>Options</b>	<i>oid</i> —Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. It can be specified either by a sequence of dotted integers or by a subtree name.  include—Include the subtree of MIB objects represented by the specified OID.  exclude—Exclude the subtree of MIB objects represented by the specified OID.
<b>Usage Guidelines</b>	See “Configuring the Trap Notification Filter” on page 64.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## parameters

---

<b>Syntax</b>	parameters { message-processing-model (v1   v2c   v3); security-model (usm   v1   v2c); security-level (none   authentication   privacy); security-name <i>security-name</i> ; }
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> ]
<b>Description</b>	Configure a set of target parameters.  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Define the Trap Target Parameters” on page 68.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## port

---

<b>Syntax</b>	port < <i>port-number</i> >;
<b>Hierarchy Level</b>	[edit snmp v3 target-address <i>target-address-name</i> ]
<b>Description</b>	Configure a UDP port number for an SNMP target.
<b>Options</b>	< <i>port-number</i> >—(Optional) Port number for an SNMP target. <b>Default:</b> port number 162
<b>Usage Guidelines</b>	See “Configuring the Port” on page 66.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## privacy-3des

---

<b>Syntax</b>	<pre>privacy-3des {     privacy-password <i>privacy-password</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ]
<b>Description</b>	Configure the triple Data Encryption Standard (3DES) for the SNMPv3 user.
<b>Options</b>	<p><i>privacy-password</i>—The password used to generate the key used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a routing platform:</p> <p style="padding-left: 40px;">The password must be at least 8 characters long.</p> <p style="padding-left: 40px;">You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.</p>
<b>Usage Guidelines</b>	See “Configuring the Encryption Type” on page 51.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

## privacy-aes128

---

<b>Syntax</b>	<pre>privacy-aes128 {     privacy-password <i>privacy-password</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ]
<b>Description</b>	Configure the Advanced Encryption Standard encryption algorithm (CFB128-AES-128 Privacy Protocol) for the SNMPv3 user.
<b>Options</b>	<p><i>privacy-password</i>—The password used to generate the key used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a routing platform:</p> <p style="padding-left: 40px;">The password must be at least 8 characters long.</p> <p style="padding-left: 40px;">You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.</p>
<b>Usage Guidelines</b>	See “Configuring the Encryption Type” on page 51.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

## privacy-des

---

<b>Syntax</b>	<pre>privacy-des {     privacy-password <i>privacy-password</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ]
<b>Description</b>	Configure Data Encryption Standard (DES) for the SNMPv3 user.
<b>Options</b>	<p><i>privacy-password</i>—The password used to generate the key used for encryption.</p> <p>SNMPv3 has special requirements when you create plain-text passwords on a routing platform:</p> <p style="padding-left: 40px;">The password must be at least 8 characters long.</p> <p style="padding-left: 40px;">You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.</p>
<b>Usage Guidelines</b>	See “Configuring the Encryption Type” on page 51.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

## privacy-none

---

<b>Syntax</b>	privacy-none;
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> ]
<b>Description</b>	Configure no encryption for the SNMPv3 user.
<b>Usage Guidelines</b>	See “Configuring the Encryption Type” on page 51.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

## privacy-password

---

<b>Syntax</b>	<code>privacy-password <i>privacy-password</i>;</code>
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine user <i>username</i> privacy-3des] , [edit snmp v3 usm local-engine user <i>username</i> privacy-aes128] , [edit snmp v3 usm local-engine user <i>username</i> privacy-des]
<b>Description</b>	Configure a privacy password for the SNMPv3 user.
<b>Options</b>	<i>privacy-password</i> —The password used to generate the key used for encryption.  SNMPv3 has special requirements when you create plain-text passwords on a routing platform:  The password must be at least 8 characters long.  You can include most character classes in a password (alphabetic, numeric, and special characters), except control characters.
<b>Usage Guidelines</b>	See “Configuring the Encryption Type” on page 51.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## read-view

---

<b>Syntax</b>	<code>read-view <i>view-name</i>;</code>
<b>Hierarchy Level</b>	[edit snmp v3 vacm access group <i>group-name</i> default-context-prefix security-model (any   usm   v1   v2c) security-level (authentication   none   privacy)]
<b>Description</b>	Associate the view with a community or a group name (SNMPv3).
<b>Options</b>	<i>view-name</i> —The name of the view to which the SNMP user group has access.
<b>Usage Guidelines</b>	See “Configuring the Read View” on page 59.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>See Also</b>	See “Configuring MIB Views” on page 54.

## security-level

---

See the following sections:

security-level (Defining Access Privileges) on page 161

security-level (Generating SNMP Notifications) on page 161

### ***security-level (Defining Access Privileges)***

<b>Syntax</b>	security-level (none   authentication   privacy);
<b>Hierarchy Level</b>	[edit snmp v3 vacm access group group-name default-context-prefix security-model (any   usm   v1   v2c)]
<b>Description</b>	Define the security level used for access privileges.
<b>Options</b>	none—No authentication and no encryption. authentication—Provides authentication but no encryption. privacy—Provides authentication and encryption.
	<b>Default:</b> none
<b>Usage Guidelines</b>	See “Configuring the Security Level” on page 57.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

### ***security-level (Generating SNMP Notifications)***

<b>Syntax</b>	security-level (none   authentication   privacy);
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]
<b>Description</b>	Configure the security level to use when generating SNMP notifications.
<b>Options</b>	none—No authentication and no encryption. authentication—Provides authentication but no encryption. privacy—Provides authentication and encryption.
	<b>Default:</b> none
<b>Usage Guidelines</b>	See “Configuring the Security Level” on page 70.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## security-model

---

See the following sections:

security-model (Access Privileges) on page 162

security-model (Group) on page 162

security-model (SNMP Notifications) on page 163

### ***security-model (Access Privileges)***

**Syntax** security-model (usm | v1 | v2c);

**Hierarchy Level** [edit snmp v3 vacm access group *group-name* default-context-prefix]

**Description** Configure a group's security model used for access privileges.

**Options** usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

**Usage Guidelines** See “Configuring the Security Model” on page 57.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

### ***security-model (Group)***

**Syntax** security-model (usm | v1 | v2c);

**Hierarchy Level** [edit snmp v3 vacm security-to-group]

**Description** Define a security model for a group.

**Options** usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

**Usage Guidelines** See “Configuring the Security Model” on page 60.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**security-model (SNMP Notifications)**

<b>Syntax</b>	security-model (usm   v1   v2c);
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]
<b>Description</b>	Configure a group's security model used with sending notifications.
<b>Options</b>	usm—SNMPv3 security model. v1—SNMPv1 security model. v2c—SNMPv2c security model.
<b>Usage Guidelines</b>	See “Configuring the Security Model” on page 70.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

**security-name**


---

See the following sections:

- security-name (Community String) on page 163
- security-name (Security Group) on page 164
- security-name (SNMP Notifications) on page 164

**security-name (Community String)**

<b>Syntax</b>	security-name <i>security-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 snmp-community <i>community-index</i> ]
<b>Description</b>	Associate the community string configured at the [edit snmp v3 snmp-community <i>community-index</i> ] hierarchy level to a security name.
<b>Options</b>	<i>security-name</i> used when performing access control.



**NOTE:** The security name must match the configured security name at the [edit snmp v3 target-parameters *target-parameters-name* parameters] hierarchy level when configuring traps.

---

<b>Usage Guidelines</b>	See “Configuring the Security Names” on page 73.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

**security-name (Security Group)**

<b>Syntax</b>	security-name <i>security-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 vacm security-to-group security-model (usm   v1  v2c)]
<b>Description</b>	Associate a group or a community string with a configured security group.
<b>Options</b>	<i>security-name</i> —The username configured at the [edit snmp v3 usm local-engine user <i>username</i> ] hierarchy level. For SNMPv1 and SNMPv2c, the security name is the community string configured at the [edit snmp v3 snmp-community <i>community-index</i> ] hierarchy level.
<b>Usage Guidelines</b>	See “Configuring the Security Name” on page 61.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

**security-name (SNMP Notifications)**

<b>Syntax</b>	security-name <i>security-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 target-parameters <i>target-parameters-name</i> parameters]
<b>Description</b>	Configure the security name used when generating SNMP notifications.
<b>Options</b>	<i>security-name</i> —If the USM security model is used, the security name identifies the user that is used when generating the notification. If the v1 or v2c security models are used, the security name identifies the SNMP community used when generating the notification.



**NOTE:** The access privileges for the group associated with this security name must allow this notification to be sent.

If you are using the v1 or v2 security models, the security name at the [edit snmp v3 vacm security-to-group] hierarchy level must match the security name at the [edit snmp v3 snmp-community *community-index*] hierarchy level.

---

<b>Usage Guidelines</b>	See “Configuring the Security Name” on page 70.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## security-to-group

---

<b>Syntax</b>	<pre>security-to-group {     security-model (usm   v1   v2c) {         security-name <i>security-name</i>;         group <i>group-name</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit snmp v3 vacm]
<b>Description</b>	<p>Configure the group to which a specific security name belongs.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “Assigning Security Names to Groups” on page 60.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

## snmp-community

---

<b>Syntax</b>	<pre>snmp-community <i>community-index</i> {     community-name <i>community-name</i>;     security-name <i>security-name</i>;     tag <i>tag-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit snmp v3]
<b>Description</b>	Configure the SNMP community.
<b>Options</b>	<p><i>community-index</i>—(Optional) String that identifies an SNMP community.</p> <p>The remaining statements are explained separately.</p>
<b>Usage Guidelines</b>	See “Configuring the SNMP Community” on page 72.
<b>Required Privilege Level</b>	<p>snmp—To view this statement in the configuration.</p> <p>snmp-control—To add this statement to the configuration.</p>

tag

---

<b>Syntax</b>	tag <i>tag-name</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 notify <i>name</i> ], [edit snmp v3 snmp-community <i>community-index</i> ]
<b>Description</b>	Configure a set of targets to receive traps (for IPv4 packets only).
<b>Options</b>	<i>tag-name</i> —Identifies the address of managers that are allowed to use a community string.
<b>Usage Guidelines</b>	See “Configuring the Tag” on page 73 and “Configuring the Trap Notification” on page 63.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

tag-list

---

<b>Syntax</b>	tag-list [ <i>tag-list</i> ];
<b>Hierarchy Level</b>	[edit snmp v3 target-address <i>target-address-names</i> ]
<b>Description</b>	Configure an SNMP tag list used to select target addresses.
<b>Options</b>	<i>tag-list</i> —Defines sets of target addresses.
<b>Usage Guidelines</b>	See “Configuring the Tag List” on page 66.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## target-address

---

**Syntax** target-address *target-address-name* {  
 address *address*;  
 address-mask *address-mask*;  
 port <*port-number*>;  
 tag-list [ *tag-list* ];  
 target-parameters *target-parameters-name*;  
 }

**Hierarchy Level** [edit snmp v3]

**Description** Configure a management application's address and parameters to be used in sending notifications.

**Options** *target-address-name*—A string that identifies the target address.

The remaining statements are explained separately.



**NOTE:** You must configure the address mask when you configure the SNMP community.

---

**Usage Guidelines** See “Configuring the Trap Target Address” on page 65.

**Required Privilege Level** snmp—To view this statement in the configuration.  
 snmp-control—To add this statement to the configuration.

## target-parameters

---

**Syntax** target-parameters *target-parameters-name* {  
 notify-filter *profile-name*;  
 parameters {  
 message-processing-model (v1 | v2c | V3);  
 security-model ( usm | v1 | v2c);  
 security-level (authentication | none | privacy);  
 security-name *security-name*;  
 }  
 }

**Hierarchy Level** [edit snmp v3]

**Description** Configure the message processing and security parameters to be used in sending notifications to a particular management target.

The remaining statements are explained separately.

**Usage Guidelines** See “Define the Trap Target Parameters” on page 68.

**Required Privilege Level** snmp—To view this statement in the configuration.  
 snmp-control—To add this statement to the configuration.

## type

---

<b>Syntax</b>	type trap ;
<b>Hierarchy Level</b>	[edit snmp v3 notify <i>name</i> ]
<b>Description</b>	Configure the type of notification.
<b>Options</b>	trap—Defines the type of notification.
<b>Usage Guidelines</b>	See “Configuring the Trap Notification” on page 63.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## user

---

<b>Syntax</b>	user <i>username</i> ;
<b>Hierarchy Level</b>	[edit snmp v3 usm local-engine]
<b>Description</b>	Specify a user associated with an SNMPv3 group.
<b>Options</b>	<i>username</i> —SNMPv3 USM username.
<b>Usage Guidelines</b>	See “Creating SNMPv3 Users” on page 49.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>Usage Guidelines</b>	See “Creating SNMPv3 Users” on page 49.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.

## usm

```

Syntax  usm {
            local-engine {
                user username {
                    authentication-md5 {
                        authentication-password authentication-password;
                    }
                    authentication-sha {
                        authentication-password authentication-password;
                    }
                    authentication-none;
                    privacy-aes128 {
                        privacy-password privacy-password;
                    }
                    privacy-des {
                        privacy-password privacy-password;
                    }
                    privacy-3des {
                        privacy-password privacy-password;
                    }
                    privacy-none {
                        privacy-password privacy-password;
                    }
                    privacy-none;
                }
            }
        }

```

**Hierarchy Level** [edit snmp v3]

**Description** Configure user-based security model (USM) information.

The remaining statements are explained separately.

**Usage Guidelines** See “Creating SNMPv3 Users” on page 49.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## vacm

```

Syntax vacm {
    access {
        group group-name {
            default-context-prefix {
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c);
        security-name security-name {
            group group-name;
        }
    }
}

```

**Hierarchy Level** [edit snmp v3]

**Description** Configure view-based access control model (VACM) information.


The remaining statements are explained separately.

**Usage Guidelines** See “Defining Access Privileges for an SNMP Group” on page 55.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

## view

---

<b>Syntax</b>	view <i>view-name</i> { oid <i>object-identifier</i> (include   exclude); }
<b>Hierarchy Level</b>	[edit snmp]
<b>Description</b>	Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The view statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the view statement at the [edit snmp community <i>community-name</i> ] hierarchy level. For SNMPv3, you must associate the view with a group name configured at the [edit snmp v3 vacm] hierarchy level.
	<b>NOTE:</b> To remove an OID completely, use the delete view all oid oid-number command but omit the include parameter.
<b>Options</b>	<i>view-name</i> —Name of the view  The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Configuring MIB Views” on page 54.
<b>Required Privilege Level</b>	snmp—To view this statement in the configuration. snmp-control—To add this statement to the configuration.
<b>See Also</b>	“Associating MIB Views with an SNMP User Group” on page 58.

---

v3

```

Syntax v3 {
    notify name {
        tag tag-name;
        type trap;
    }
    notify-filter profile-name {
        oid object-identifier (include | exclude);
    }
    snmp-community community-index {
        security-name community-name;
        security-name security-name;
        tag tag-name;
    }
    target-address target-address-name {
        address address;
        address-mask address-mask;
        port <port-number>;
        tag-list [ tag-list ];
        target-parameters target-parameters-name;
    }
    target-parameters target-parameters-name {
        notify-filter profile-name;
        parameters {
            message-processing-model (v1 | v2c | V3);
            security-model ( usm | v1 | v2c);
            security-level (authentication | none | privacy);
            security-name security-name;
        }
    }
    usm {
        local-engine {
            user username {
                authentication-md5 {
                    authentication-password authentication-password;
                }
                authentication-sha {
                    authentication-password authentication-password;
                }
                authentication-none;
                privacy-aes128 {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-des {
                    privacy-password privacy-password;
                }
                privacy-none;
            }
        }
    }
}

```

```

vacm {
  access {
    group group-name {
      default-context-prefix {
        security-model (any | usm | v1 | v2c) {
          security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
          }
        }
      }
    }
  }
}
security-to-group {
  security-model (usm | v1 | v2c) {
    security-name security-name {
      group group-name;
    }
  }
}
}

```

**Hierarchy Level** [edit snmp]

**Description** Configure SNMPv3.

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring SNMPv3” on page 45.

**Required Privilege Level** snmp—To view this statement in the configuration.

## write-view

---

**Syntax** write-view *view-name*;

**Hierarchy Level** [edit snmp v3 vacm access group *group-name* default-context-prefix security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

**Description** Associate the view with a community or a group name (SNMPv3).

**Options** *view-name*—The name of the view to which the SNMP user group has access.

**Usage Guidelines** See “Configuring the Write View” on page 59.

**Required Privilege Level** snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

**See Also** See “Configuring MIB Views” on page 54.

