

# Contents

Introduction .....	1
Prerequisites .....	1
Example: Configuring SNMPv1 or SNMPv2c .....	1
Network configuration .....	1
Applicable hardware and software versions .....	1
Restrictions and guidelines .....	3
Procedures .....	3
Configuring the SNMP agent .....	3
Configuring the NMS .....	4
Verifying the configuration .....	5
Configuration files .....	5
Example: Configuring SNMPv3 .....	6
Network configuration .....	6
Applicable hardware and software versions .....	6
Restrictions and guidelines .....	8
Procedures .....	8
Configuring the SNMP agent in RBAC mode .....	8
Configuring the SNMP agent in VACM mode .....	9
Configuring the NMS .....	9
Verifying the configuration .....	11
Configuration files .....	11
SNMPv3 configuration in RBAC mode .....	11
SNMPv3 configuration in VACM mode .....	12

# Introduction

This document provides SNMP configuration examples.

## Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

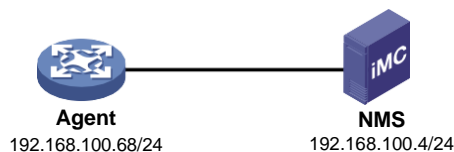
This document assumes that you have basic knowledge of SNMP.

## Example: Configuring SNMPv1 or SNMPv2c

### Network configuration

As shown in [Figure 1](#), an INC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv1/SNMPv2c to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS.

**Figure 1 Network diagram**



# Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Restrictions and guidelines

When you configure SNMPv1 or SNMPv2c, follow these restrictions and guidelines:

- The configuration procedure is the same for SNMPv1 and SNMPv2c. This example uses SNMPv2c.
- For the NMS to manage the SNMP agent, the SNMP settings on the agent and the NMS must match.
- The NMS software configuration varies by vendor. This example uses the INC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.

## Procedures

### Configuring the SNMP agent

# Specify SNMPv2c, and create read-only community **readtest** and read and write community **writetest**.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

# Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

# Enable SNMP notifications, specify the NMS at 192.168.100.4 as the SNMP trap destination, and use **readtest** as the community name.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest v2c
```

# Configuring the NMS

1. Add the device (SNMP agent) to the INC:
  - a. Click the **Resource** tab.
  - b. From the navigation tree, select **Resource Management > Add Device**.
  - c. On the **Add Device** page, configure the following parameters:
    - Enter **192.168.100.68** in the **Host Name/IP** field.
    - Use the default values for other parameters.

**Figure 2 Adding a device**

Resource > Add Device

**Basic Information**

Host Name/IP \* 192.168.100.68

Device Label

Mask

Device Group

Login Type Telnet

☒ Automatically register to receive SNMP traps from supported devices

☒ Support Ping Operation

☐ Add the device regardless of the ping result

☐ Use the loopback address as the management IP

**SNMP Settings**

**Configure**

Parameter Type	SNMPv2c
Read-Only Community String	*****
Read-Write Community String	*****
Timeout (seconds)	4
Retries	3

**Telnet Settings**

**SSH Settings**

OK Cancel

2. Configure SNMP parameters:
  - a. Expand the **SNMP Settings** area.
  - b. Click **Configure**.
  - c. On the page that appears, configure the following parameters:
    - Select **SNMPv2c** from the **Parameter Type** list.
    - Enter **readtest** in the **Read-Only Community String** field.
    - Enter **writetest** in the **Read-Write Community String** field.

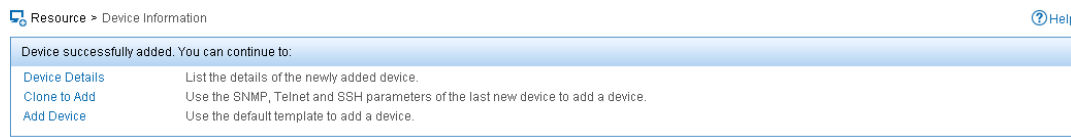
- Use the default values for other parameters.
- Click **OK**.

**Figure 3 Configuring SNMP parameters**

3. On the **Add Device** page, click **OK**.

The device is successfully added to the INC, as shown in [Figure 4](#).

**Figure 4 Device added**



## Verifying the configuration

1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
  - a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
  - b. Click the **Alarm** tab.
  - c. From the navigation tree, select **Alarm Browse > All Alarms**.

## Configuration files

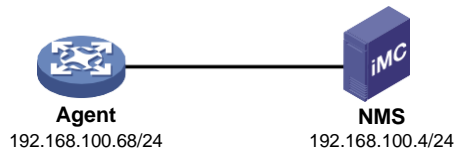
```
#
snmp-agent
snmp-agent community write writetest
snmp-agent community read readtest
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v2c
snmp-agent trap enable arp
snmp-agent trap enable syslog
snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest v2c
#
```

# Example: Configuring SNMPv3

## Network configuration

As shown in [Figure 5](#), an INC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv3 to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS.

**Figure 5 Network diagram**



# Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Restrictions and guidelines

When you configure SNMPv3, follow these restrictions and guidelines:

- SNMPv3 supports VACM and RBAC access control modes. This example provides SNMPv3 configuration procedures in both modes. See "[Configuring the SNMP agent in RBAC mode](#)" and "[Configuring the SNMP agent in VACM mode](#)".
- For the NMS to manage the SNMP agent, the SNMP settings on the agent and the NMS must match.
- The NMS software configuration varies by vendor. This example uses the INC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.
- For the NMS to receive notifications from the agent, make sure the following configurations are the same on the NMS and the SNMP agent:
  - SNMPv3 username.
  - SNMP protocol version.
  - Authentication algorithm.
  - Privacy algorithm.
  - Authentication and privacy keys.

## Procedures

### Configuring the SNMP agent in RBAC mode

```
# Enable SNMPv3.
```

```
<Agent> system-view
```

```
[Agent] snmp-agent sys-info version v3
```

```
# Create user role test, and assign test read and write access to the objects under the internet subtree (OID: 1.3.6.1).
```

```
[Agent] role name test
```

```
[Agent-role-test] rule 1 permit read write oid 1.3.6.1
```

```
[Agent-role-test] quit
```

# Create SNMPv3 user **managev3user**. Assign user role **test** to **managev3user**. Set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encryption key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 managev3user user-role test simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

# Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
```

```
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

# Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

# Specify the NMS at **192.168.100.4** as the trap destination, and set the username to **managev3user** for the traps.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

## Configuring the SNMP agent in VACM mode

# Enable SNMPv3.

```
<Agent> system-view
```

```
[Agent] snmp-agent sys-info version v3
```

# Include the **mib-2** (OID 1.3.6.1) subtree in the **mibtest** view.

```
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```

# Create SNMPv3 group **managev3group**, and specify the authentication with privacy security model for the group. Assign the group read, write, and notification accesses to the **mibtest** view.

```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view mibtest
```

# Add user **managev3user** to SNMPv3 group **managev3group**, and set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encryption key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

# Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
```

```
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

# Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

# Specify the NMS at **192.168.100.4** as the trap destination, and set the username to **managev3user** for the traps.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

## Configuring the NMS

1. Add an SNMP template:
  - a. Click the **System** tab.
  - b. From the navigation tree, select **Resource Management > SNMP Template**.
  - c. On the **SNMP Template** page, click **Add**.
  - d. On the **Add SNMP Template** page, configure the following parameters:



- Enter **SNMPv3** in the **Name** field.
- Select **SNMPv3 Priv-Aes128 Auth-Sha** from the **Parameter Type** list.
- Enter **managev3user** in the **Username** field.
- Enter **123456TESTauth&!** in the **Authentication Password** field.
- Enter **123456TESTencr&!** in the **Encryption Password** field.
- Use the default values for other parameters.
- Click **OK**.

**Figure 6 Adding an SNMP template**

2. Add the device (SNMP agent) to INC:
  - a. Click the **Resource** tab.
  - b. From the navigation tree, select **Resource Management > Add Device**.
  - c. On the **Add Device** page, configure the following parameters:
    - Enter **192.168.100.68** in the **Host Name/IP** field.
    - Use the default values for other parameters.

**Figure 7 Adding a device**

3. Configure SNMP parameters:
  - a. Expand the **SNMP Settings** area.
  - b. Click **Configure**.

- c. Select the **Select an Existing Template** option.
- d. Select template name **SNMPv3**.
- e. Click **OK**.

**Figure 8 Selecting an existing template**

☐ Edit SNMP Parameters
 ☒ Select an Existing Template
 Refresh

	Name	Parameter Type	Username	Timeout (seconds)	Retries
<input type="radio"/>	default	SNMPv2c		4	3
<input checked="" type="radio"/>	SNMPv3	SNMPv3 Priv-Aes128 Auth-Sha	managev3user	4	3

1-2 of 2. Page 1 of 1.

OK Cancel

4. On the **Add Device** page, click **OK**.  
The device is successfully added to INC, as shown in [Figure 9](#).

**Figure 9 Device added**

Resource > Device Information Help

Device successfully added. You can continue to:

<a href="#">Device Details</a>	List the details of the newly added device.
<a href="#">Clone to Add</a>	Use the SNMP, Telnet and SSH parameters of the last new device to add a device.
<a href="#">Add Device</a>	Use the default template to add a device.

## Verifying the configuration

1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
  - a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
  - b. Click the **Alarm** tab.
  - c. From the navigation tree, select **Alarm Browse > All Alarms**.

## Configuration files

### SNMPv3 configuration in RBAC mode

```
#
snmp-agent
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v3
snmp-agent trap enable arp
snmp-agent trap enable syslog
snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

```

snmp-agent usm-user v3 managev3user user-role test cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRwdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
role name test
rule 1 permit read oid 1.3.6.1
#

```

## SNMPv3 configuration in VACM mode

```

#
snmp-agent
snmp-agent sys-info contact Mr.Wang-Tel:3306
snmp-agent sys-info location telephone-closet,3rd-floor
snmp-agent sys-info version v3
snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest
notify-view mibtest
snmp-agent mib-view included mibtest internet
snmp-agent trap enable arp
snmp-agent trap enable syslog

snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRwdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#

```