# Exclude OID in Nexus 5k,7k and 9K in SNMP v2 and v3 Configuration

## Contents



## Introduction

This document describes how to exclude OID in Nexus 5k, 7k, and 9K in SNMP v2 and v3 configuration.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics before implementing Object Identifier (OID) exclusions:

- Familiarity with Simple Network Management Protocol (SNMP)
- Access to device configuration mode
- Understanding of OIDs to be excluded
- Understanding of SNMP community and user configurations

### Components Used

The information in this document is based on the Lab test with these Nexus models:

- Nexus 5k
- Nexus 7k
- Nexus 9k

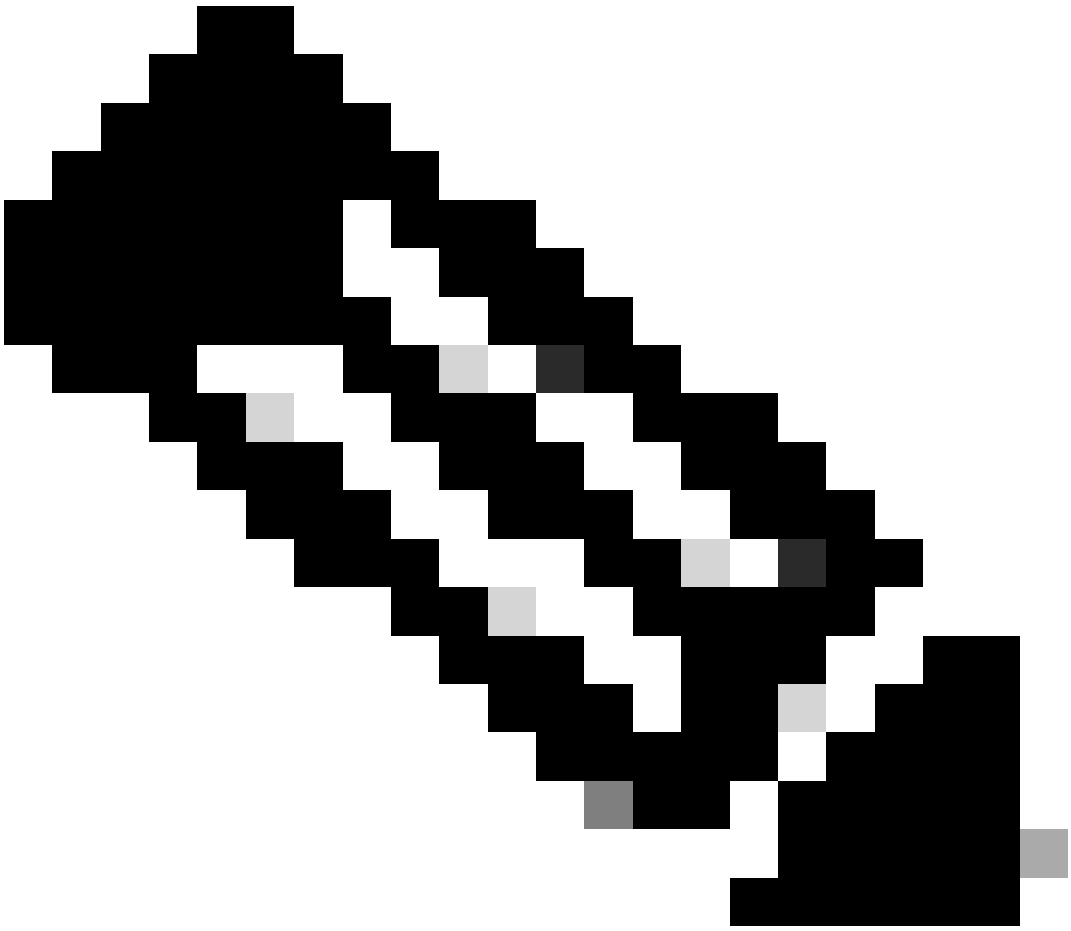
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

In the world of SNMP, you often encounter situations where the parsing of the Management Information Base (MIB) tree faces hurdles, reaching a standstill at specific OIDs sometimes leading to window timeouts or similar issues. Another common challenge arises when continuous polling for a troublesome OID triggers

alerts that are neither necessary nor impactful. One possible way to get rid of these kinds of scenarios is you create exclusions, instructing the device to skip that specific OID and proceed with the rest of the MIB structure. By directing the device to bypass the troublesome OID and proceed with the remainder of the MIB structure, you can foster a smooth flow of the MIB tree.

---



> **Note**: It is important to note that this exclusion can affect how we read data from the MIB tree. Exercise caution and ensure the necessity of the OID before proceeding with these exclusions.

---

While the exclusion of OIDs typically pursues a straightforward process in devices like Aggregation Services Router (ASR)/ Catalyst switches (CAT)/Integrated Service Router (ISR), navigating this challenge in Nexus devices proves to be more intricate due to the absence of views. This article delves into an innovative approach by introducing roles and mapping them to the community/user, presenting a solution for excluding OIDs in SNMP v2 and v3 configurations on Nexus 5k, 7k, and 9K devices.

## Basic Steps

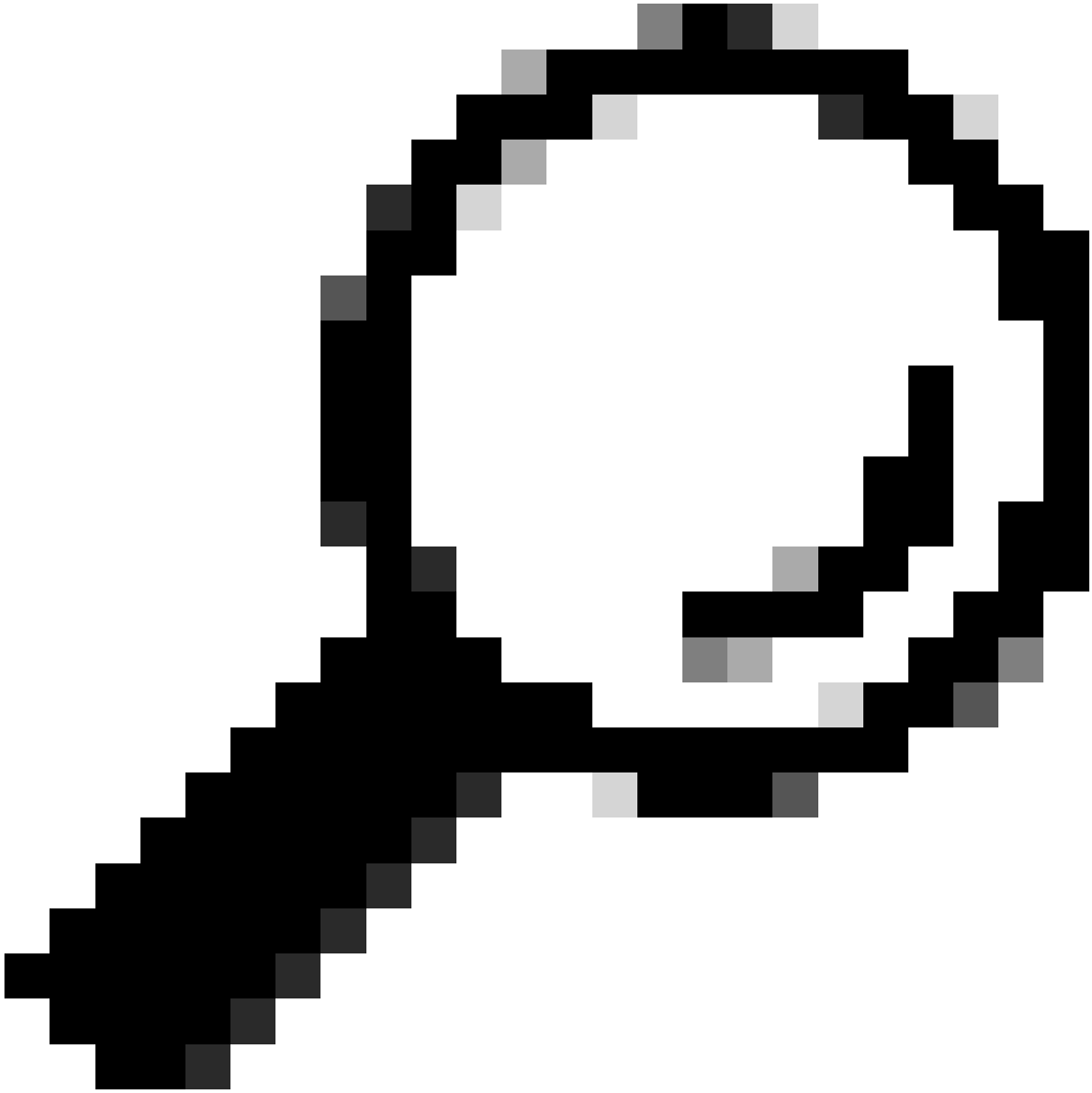
Access Configuration Mode:

```
#conf t
```

Define the Role of OID Exclusion:

```
#role name <name_of_role>
#rule 1 permit read feature snmp
#rule 2 deny {read/ read-write} oid <oid_you_want_to_exclude>
```

---



**Tip**: {read/ read-write} allows you to choose between 'read' and 'read-write' SNMP operations. 'Read' operations typically involve retrieving information, while 'read-write' operations involve both retrieving and modifying information. You can choose read/read-write as per your preference.

---

Exit Configuration Mode:

```
#exit
```

Apply Configuration to SNMP Community/User.

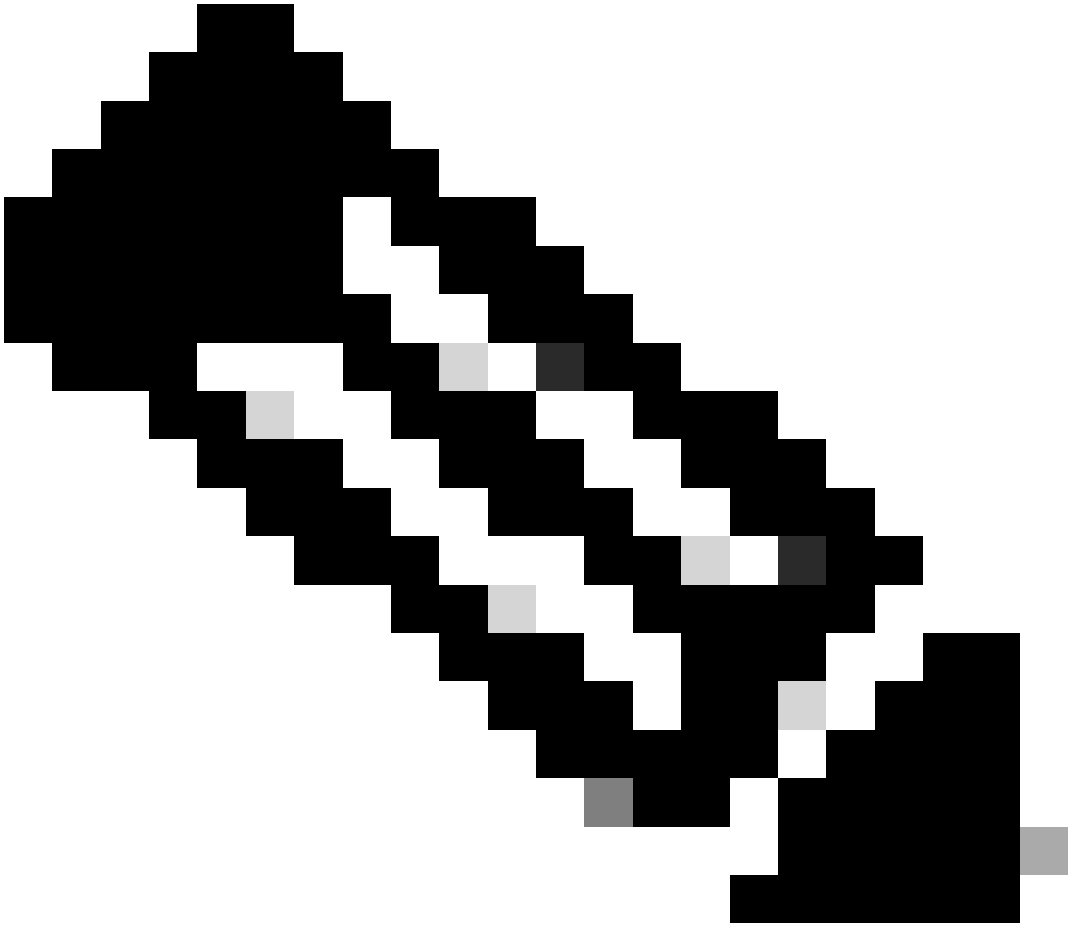
For SNMPv2:

```
#snmp-server community <name_of_community_you_want_to_map> group <name_of_role>
```

For SNMPv3:

```
#snmp-server user <user_to_map_with> <name_of_role> auth {sha/md5} <authentication_password> priv {aes/
```

# Configuration



**Note**: This example includes the exclusion of OID 1.3.6.1.2.1.2.2.1.3 (ifType). Ensure to replace the ifType OID with the one you want to exclude.

---

Defining a role to exclude OID ifType:

```
switch#
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# role name deny_oid
switch(config-role)# rule 1 permit read feature snmp
switch(config-role)# rule 2 deny read oid 1.3.6.1.2.1.2.2.1.3
switch(config-role)# exit
switch(config)# exit
switch# sh role name deny_oid
Role: deny_oid
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
```

```
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  2       deny    read        oid                 1.3.6.1.2.1.2.2.1.3
  1       permit  read        feature             snmp
switch#
```

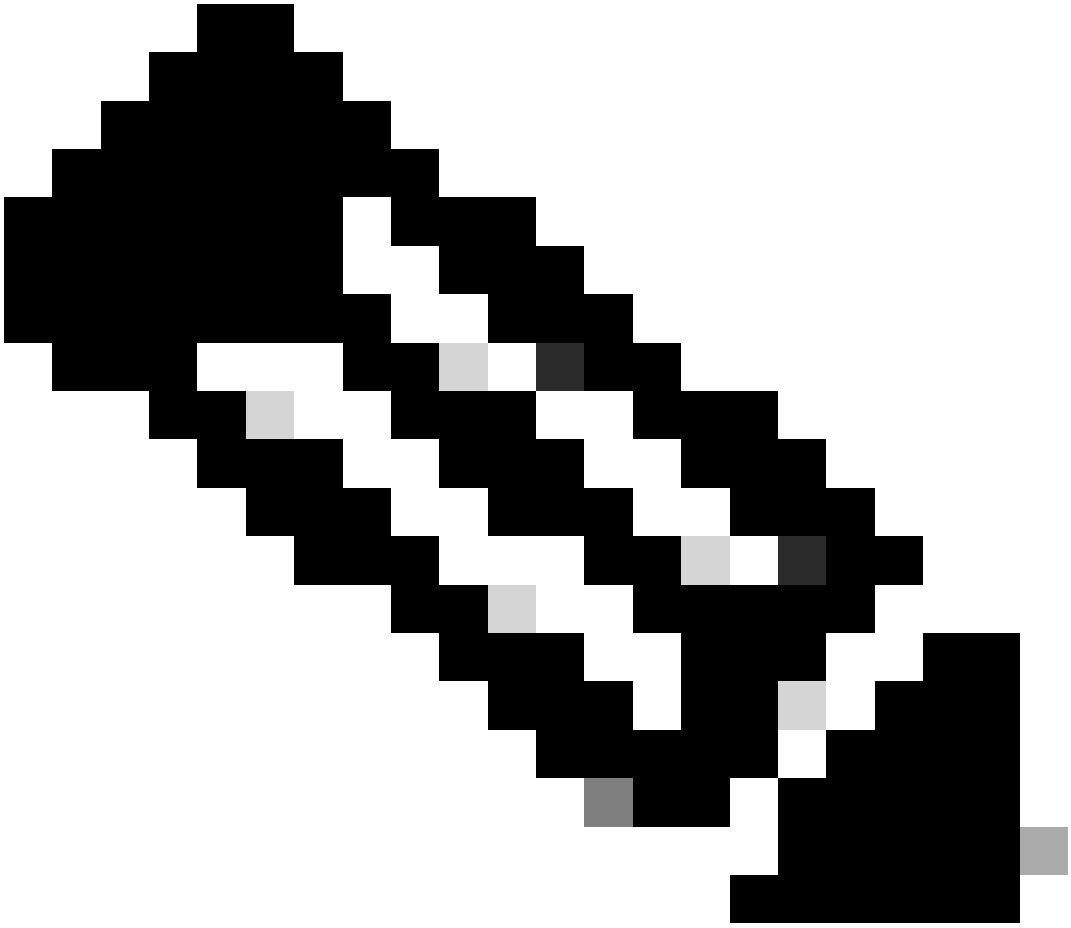
Creating an SNMPv2 community with deny_oid role:

```
switch(config)# snmp-server community snmpv2user group deny_oid
switch(config)# exit
switch# sh snmp community
Community             Group / Access      context    acl_filter
_________             ______________      _______    __________
snmpv2user            deny_oid
switch#
```

Creating SNMPv3 user with **deny_oid** role:

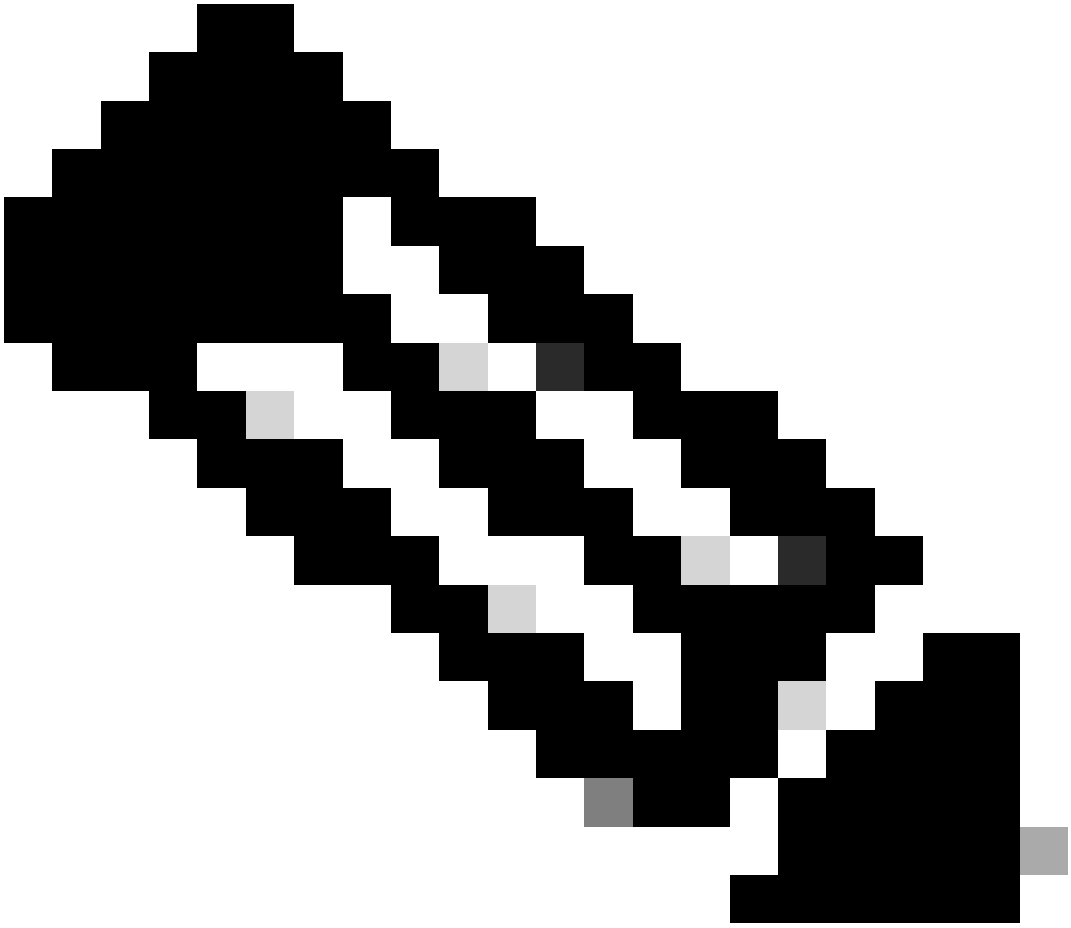
```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server user snmpv3user deny_oid auth sha password!123 priv ?
  WORD  Privacy password for user (Max Size 134)
switch(config)# snmp-server user snmpv3user deny_oid auth sha password!123 priv password!123
switch(config)# do sh snmp user
_____________________________________________________________
                  SNMP USERS
_____________________________________________________________

User                Auth      Priv(enforce) Groups              acl_filter
____                ____      ____________  ______              __________
admin               md5       aes-128(no)   network-admin
snmpv3user          sha       aes-128(no)   deny_oid
_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________
User                            Auth      Priv
___                             ____      ____
switch(config)#
```

# Verification



**Note**: A test user 'trial' was used in order to check the polling of ifType OID. The rest of the users were mapped with the **deny_oid** role and it showed no data for ifType OID as illustrated.

SNMPwalk without exclusion:



**Note**: a.b.c.d is used in place of  IP address of the device in the whole article.

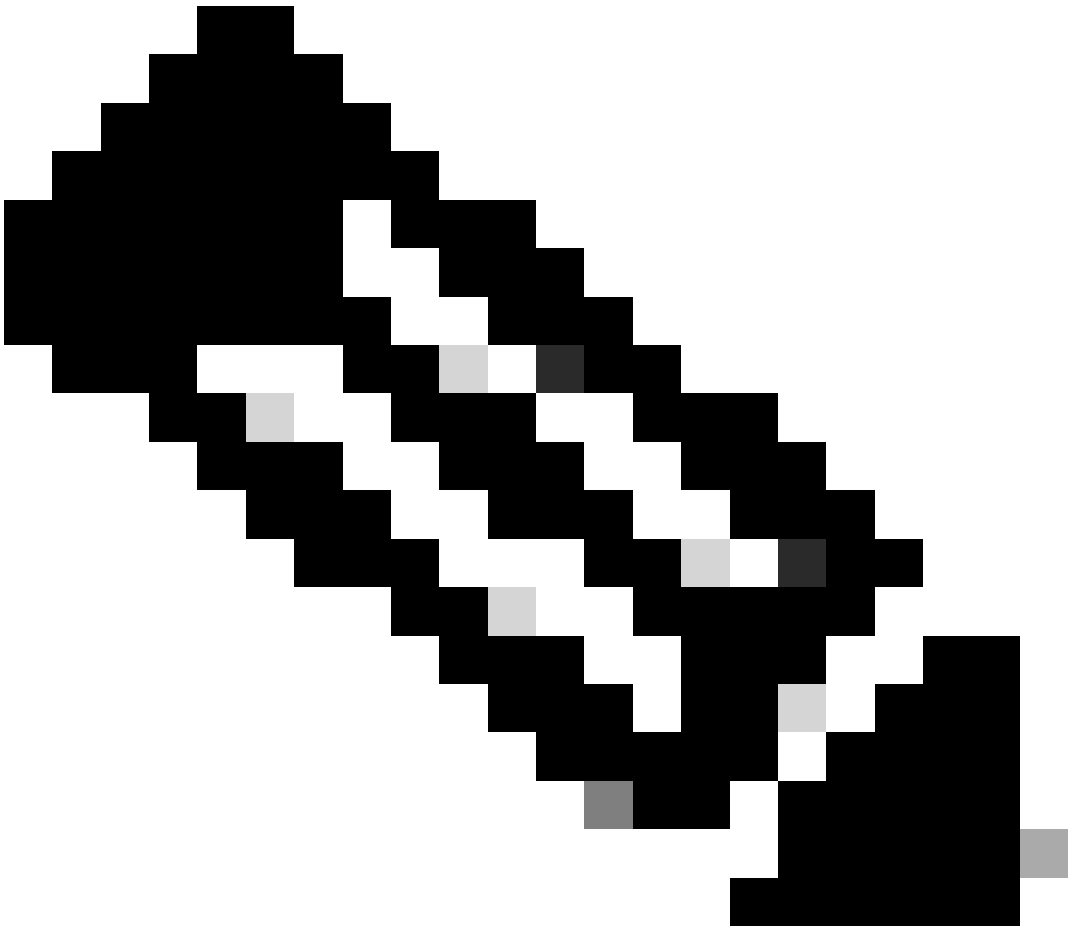
```
[root@user ~]# snmpwalk -v2c -c trial a.b.c.d 1.3.6.1.2.1.2.2.1.3
IF-MIB::ifType.83886080 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436207616 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208128 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208640 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209152 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209664 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210176 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210688 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211200 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211712 = INTEGER: ethernetCsmacd(6)
^C
```

SNMPwalk for SNMPv2 with excluded OID:

```
[root@user ~]# snmpwalk -v2c -c snmpv2user a.b.c.d 1.3.6.1.2.1.2.2.1.3
```

```
IF-MIB::ifType = No Such Object available on this agent at this OID
```

---



> **Note**: A new user 'trialv3' was created in order to illustrate polling without the exclusion of the OID.

---

SNMPwalk without excluding the OID:

```
[root@user ~]# snmpwalk -v3 -u trialv3 -l authPriv -a sha -A 'password!123' -x aes -X 'password!123' a.
IF-MIB::ifType.83886080 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436207616 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208128 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436208640 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209152 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436209664 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210176 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436210688 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211200 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436211712 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.436212224 = INTEGER: ethernetCsmacd(6)
```

```
^C
[root@user  ~]#
```

SNMPwalk for SNMPv3 user with excluded OID:

```
[root@user ~]# snmpwalk -v3 -u snmpv3user -l authPriv -a sha -A 'password!123' -x aes -X 'password!123'
IF-MIB::ifType = No Such Object available on this agent at this OID
[root@user ~]#
```