

Setup Cisco SNMPv3 via CLI:

This is for Basic setup. If the customer is looking for a more secure setup, they will need to contact Cisco. This document was only designed to get the device monitored and to troubleshoot any Issues.

Reference: [SNMPv3](#)

1. *Command:* Enable
2. *Command:* Config T
3. Create the View
 - a. *Command:* SNMP-Server view **TestSNMPv3View** Internet included
 - b. *ASA Command does not exist, this will default to standard view*
TestSNMPv3View is the View Name
If you see %Bad OID, then Internet does not exist, use ISO (if exists), or 1.3.6
 - i. Included MIB Family is included in the view
 - ii. Excluded MIB Family is excluded from the view
4. Create the Group
 - a. *Command:* SNMP-Server group **TestSNMPv3Group** v3 **priv** **Read** **TestSNMPv3View** **Write**
TestSNMPv3View
 - b. *Command (ASA Only):* SNMP-Server group **TestSNMPv3Group** v3 **priv** **Read**
TestSNMPv3Group is the Group Name
 - i. **v1**: Group using the v1 security model
 - ii. **v2c**: Group using the v2c security model
 - iii. **v3**: Group using the User security model (SNMPv3)
 - iv. **Auth**: Group using the authNoPriv Security Model
 - v. **Noauth**: Group using the noAuthNoPriv Security Model
 - vi. **Priv**: Group using the authPriv Security Model
 - vii. **Access**: Specify an access-list associated with this group
 - viii. **Context**: Specify a context to associate these views for the group
 - ix. **Notify**: Specify a notify view for the Group – Send a syslog every time a view is touched
 - x. **Read**: Specify a read view for the group
 - xi. **Write**: Specify a write view for the group
5. Create a User
 - a. *Command (same for ASA):* SNMP-Server user **TestSNMPv3User** **TestSNMPv3Group** v3 **auth** **md5** P@\$w0rd **priv** **DES** P@\$w0rd
TestSNMPv3User is the User Name
 - i. **Remote**: Specify a remote SNMP entity to which the user belongs
 - ii. **v1**: Group using the v1 security model
 - iii. **v2c**: Group using the v2c security model
 - iv. **v3**: Group using the User security model (SNMPv3)
 - v. **Access**: Specify an access-list associated with this group
 - vi. **Auth**: Authentication parameters for the user
 - vii. **Encrypted**: Specifying passwords as MD5 or SHA digests
 - viii. **MDS**: Use HMAC MD5 algorithm for authentication

- ix. **SHA**: Use HMAC SHA algorithm for authentication
- x. **3DES**: Use 168 bit 3DES algorithm for encryption
- xi. **AES**: Use AES algorithm for encryption
- xii. **DES**: Use 56 bit DES algorithm for encryption

6. Send to Destination Host (ASA Only)

- a. Command (ASA Only): SNMP-Server Host **inside** **10.10.1.1** version 3 **TestSNMPv3Group**

Note: 10.10.1.1 is the destination host that is able to monitor the Device, if the IP Address of Solarwinds NPM is not in the list, then you will not be able to add the Device

- i. **inside** Name of interface Vlan1
- ii. **outside** Name of interface Vlan2

7. Example of the configuration from start to finish:

- a. Standard Cisco:

```
Cisco:enable
Cisco#config t
Enter configuration commands, one per line. End with CNTL/Z.

Cisco(config)#SNMP-Server view TestSNMPv3View internet included
Cisco(config)#SNMP-Server group TestSNMPv3Group v3 priv Read TestSNMPv3View Write
TestSNMPv3View
Cisco(config)#SNMP-Server user TestSNMPv3User TestSNMPv3Group v3 auth MD5 P@$w0rd
priv DES P@$w0rd
```

- b. Cisco ASA:

```
Cisco:enable
Cisco#config t

Cisco(config)# SNMP-Server group TestSNMPv3Group v3 priv
Cisco(config)# SNMP-Server user TestSNMPv3User TestSNMPv3Group v3 auth MD5 P@$w0rd
priv DES P@$w0rd
Cisco(config)# SNMP-Server Host inside 10.10.1.1 version 3 TestSNMPv3User
```

8. Adding the device in Orion:

Note: Do not initially add Read/Write Credentials, then select Test.

Most Devices: SNMP and ICMP
Recommended for most devices to collect variety of data including CPU, memory, volumes, status, response time

SNMP Version: SNMPv3 is a secure version
SNMP Port:
☐ Allow 64 bit counters

SNMPv3 Credentials
SNMPv3 Username:
SNMPv3 Context:

SNMPv3 Authentication
Method:
Password: ☐ Password is a key

SNMPv3 Privacy / Encryption
Method:
Password: ☐ Password is a key

Credential Set Library
Name:
Saved Credential Sets:

Read / Write SNMPv3 Credentials
SNMPv3 Username:
SNMPv3 Context:

SNMPv3 Authentication
Method:
Password: ☐ Password is a key

SNMPv3 Privacy / Encryption
Method:
Password: ☐ Password is a key

Credential Set Library
Name:
Saved Credential Sets:

☒ Test Successful!

SNMPv3 Traps (Orion Core 2011.2 and higher)

Note: This assumes that you have setup and configured SNMPv3 on the device already.

1. Add the following while in Configuration Terminal:
 - a. *Command:* snmp-server host 10.10.1.6 version 3 auth [TestSNMPv3User](#)
 - i. *The authentication must match the same as the SNMPv3 configuration*
1. You can add the following on the same command line to generate Traps:

config syslog aaa_server snmp (these are basic Trap types sent.)

Troubleshooting SNMPv3 Traps.

1. Check the Log File:
 - a. Server 2008:
 - i. C:\ProgramData\Solarwinds\Logs\Orion\TrapService.log
 - b. Server 2003
 - i. C:\Documents and Settings\All Users\Application Data\Solarwinds\Logs\Orion\TrapService.log
2. If you see the following Error please see [This KB](#)

```
ERROR TrapService.TrapService - Bad trap packet received from Node with  
IP <IP of Device>. Error description : Security level is set to 2 but  
no encryption password was provided.
```

Wireless:

Add to your current View:

- a. *Command:* SNMP-Server view [TestSNMPv3View](#) **ieee802dot11** included

Network Topology and the UDT Module for VLANs:

While everything works by default on SNMPv2, you will need to add new commands to the Cisco devices to expose per VLAN values for this MIB. According to Cisco, SNMPv2 and SNMPv3 work quite differently when polling the BRIDGE-MIB which contains these layer 2 values. There is no single command that will expose all existing VLANs. If on a certain switch you have devices on VLANs 3, 10, and 41, you needed to add the following commands to assign them to the group:

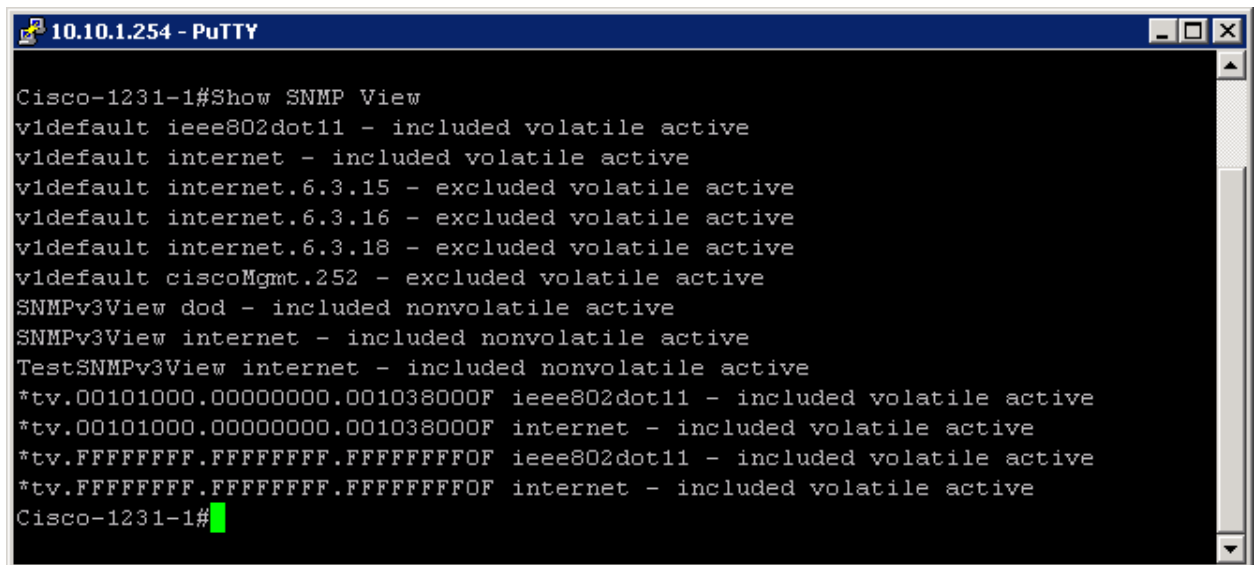
- a. *Command:* snmp-server group [TestSNMPv3Group](#) v3 priv context vlan-3
- b. *Command:* snmp-server group [TestSNMPv3Group](#) v3 priv context vlan-10
- c. *Command:* snmp-server group [TestSNMPv3Group](#) v3 priv context vlan-41

2. **Important Commands** to use to **Remove existing configurations**, please use ? for more options:

- a. No snmp-server group
- b. No snmp-server user
- c. No snmp-server host

3. **Command:** Show snmp view

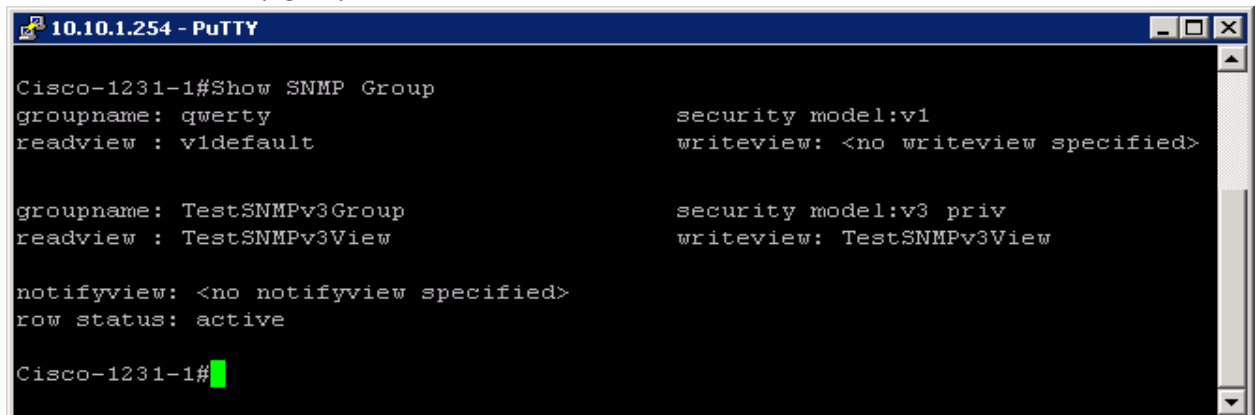
- a. Views - contained in groups
 - i. Views define what MIBs are available on the Device



```
10.10.1.254 - PuTTY
Cisco-1231-1#Show SNMP View
vldfault ieee802dot11 - included volatile active
vldfault internet - included volatile active
vldfault internet.6.3.15 - excluded volatile active
vldfault internet.6.3.16 - excluded volatile active
vldfault internet.6.3.18 - excluded volatile active
vldfault ciscoMgmt.252 - excluded volatile active
SNMPv3View dod - included nonvolatile active
SNMPv3View internet - included nonvolatile active
TestSNMPv3View internet - included nonvolatile active
*tv.00101000.00000000.00103800F ieee802dot11 - included volatile active
*tv.00101000.00000000.00103800F internet - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFFOF ieee802dot11 - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFFOF internet - included volatile active
Cisco-1231-1#
```

- ii. The view name we are looking for here is TestSNMPv3View, and you can see it includes everything from Internet down
- iii. MIB Iso is 1. and below

4. **Command:** Show snmp group



```
10.10.1.254 - PuTTY
Cisco-1231-1#Show SNMP Group
groupname: qwerty                security model:v1
readview : vldfault              writeview: <no writeview specified>

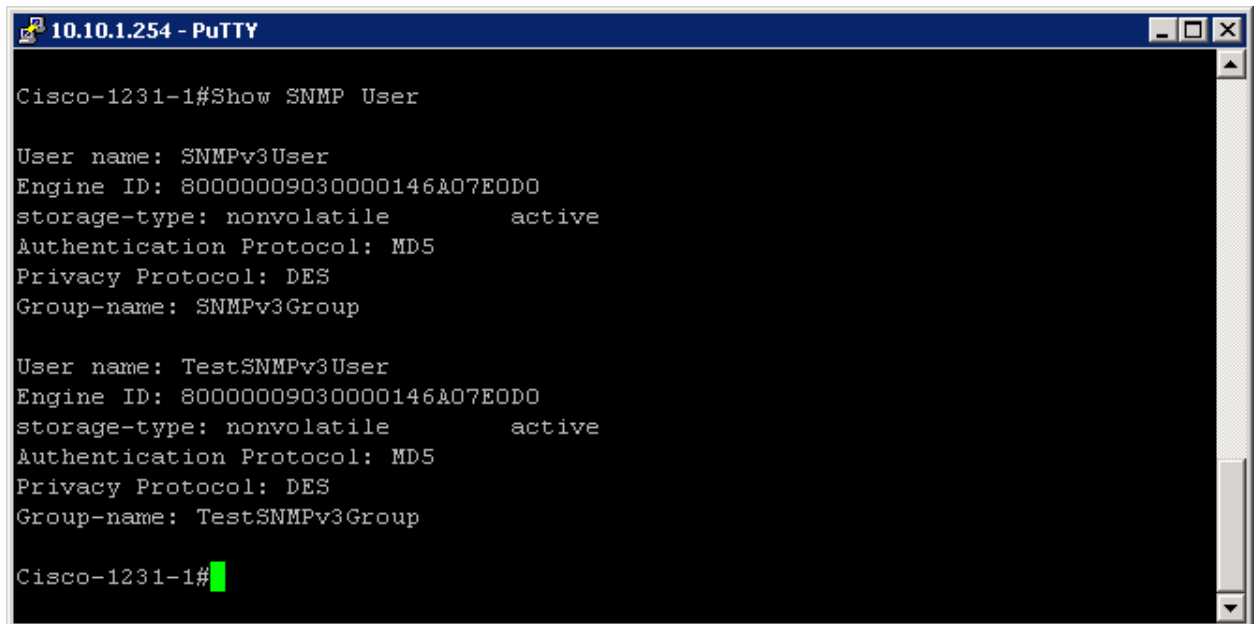
groupname: TestSNMPv3Group       security model:v3 priv
readview : TestSNMPv3View        writeview: TestSNMPv3View

notifyview: <no notifyview specified>
row status: active

Cisco-1231-1#
```

- a. Group view associates from the TestSNMPv3Group is the following:
 - i. Read view: TestSNMPv3View
 - ii. Write View: TestSNMPv3View
 - iii. Security Model: v3 priv

5. Command: show snmp user



```
Cisco-1231-1#Show SNMP User

User name: SNMPv3User
Engine ID: 80000009030000146A07E0D0
storage-type: nonvolatile      active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: SNMPv3Group

User name: TestSNMPv3User
Engine ID: 80000009030000146A07E0D0
storage-type: nonvolatile      active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: TestSNMPv3Group

Cisco-1231-1#
```

- a. Looking at the User TestSNMPv3User, it is assigned to the group TestSNMPv3Group.

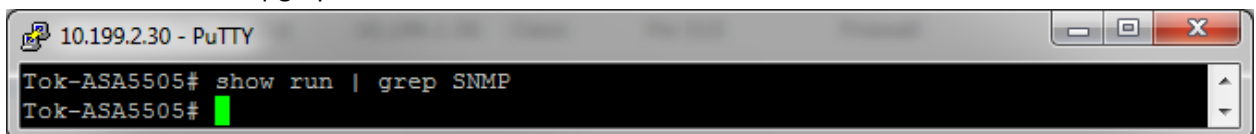
Troubleshooting an ASA

Note: Show SNMP View does not work on ASA Devices, you will use def_read_view as the view



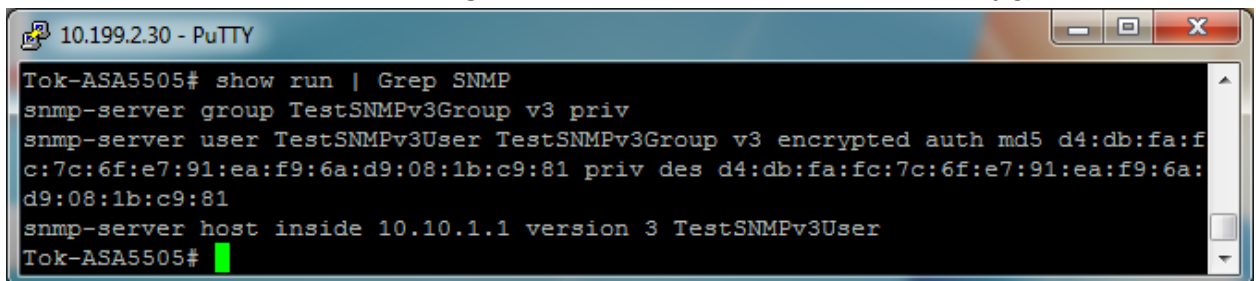
```
Tok-ASA5505# show snmp view
ERROR: % Invalid input detected at '^' marker.
Tok-ASA5505#
```

1. Command: Show run | grep SNMP



```
Tok-ASA5505# show run | grep SNMP
Tok-ASA5505#
```

- a. Shows the current SNMP Configuration (*note none is listed, so this is no config*)



```
Tok-ASA5505# show run | Grep SNMP
snmp-server group TestSNMPv3Group v3 priv
snmp-server user TestSNMPv3User TestSNMPv3Group v3 encrypted auth md5 d4:db:fa:f
c:7c:6f:e7:91:ea:f9:6a:d9:08:1b:c9:81 priv des d4:db:fa:fc:7c:6f:e7:91:ea:f9:6a:
d9:08:1b:c9:81
snmp-server host inside 10.10.1.1 version 3 TestSNMPv3User
Tok-ASA5505#
```

- b. Shows the current SNMP Configuration. Note that this is the exact same configuration as in step 7, and the password is encrypted.
- c. Also Note the Host and the Interface it is going out on