How To | How to configure SNMPv3 on Allied Telesyn devices

Introduction

This document describes how to configure Simple Network Management Protocol v3 (SNMPv3) on Allied Telesyn devices. When SNMP was first introduced security was not really a consideration, but as its use increased several security weaknesses became apparent. SNMPv3 was introduced to attempt to address those weaknesses. There are two major areas of enhancement:

- Authentication
- Privacy

What information will you find in this document?

Sections include:

Which product and software version does this information apply to?

The information provided in this document applies to:

- **Products**: AR400 Series, AR700 Series, Rapier Series, AT-8600 Series, AT-8700 Series, AT-8800 Series, AT-8900 Series, AT-9800 Series, AT-9900 Series, SwitchBlade.
- **Software releases**: v2.6.4 and above

Configuring SNMPv3 on Allied Telesyn devices

Overview of SNMPv3

When SNMP was first introduced security was not really a consideration, but as its use increased several security weaknesses became apparent. SNMPv3 was introduced to attempt to address those weaknesses. There are two major areas of enhancement:

Authentication - By introducing time-stamping and password hashing SNMP has been made more secure, and there is much less chance of an unauthorised access of an SNMP enabled device from an Network Management Station (NMS).

Privacy - There is now the option of encryption for SNMP messages sent across a network. This ensures message integrity and prevents intercepted SNMP packets from being deciphered by unauthorised users.

In terms of configuration, these two security areas are grouped together into a "Security Level". There are three possible values for each Security Level:

- NoAuthNoPriv(No Authentication and no Privacy)
- AuthNoPriv(Authentication but no Privacy)
- AuthPriv(Authentication and Privacy)

It is now also possible with SNMPv3 to define SNMP views, groups and users to provide access control to SNMP devices, and restrict some users so they can only access the parts of the Management Information Base (MIB) that they have been given access rights to. SNMP views, groups and users are explained further below.

SNMP MIB views

An SNMP MIB view is a defined list of objects within the MIB that can be used to control what parts of the MIB can be accessed by users belonging to the SNMP group that is associated with that particular view. Objects in the view may be from anywhere in the MIB, and do not need to be in the same sub-tree. Once you have defined your views you will need to configure in your SNMP Groups the type of access users will have to those views. There are three possible types of access and at least one must be configured for the users in that SNMP group to have access to an SNMP view. The three types of configurable access are:

1. ReadView (Specifies SNMP view the group has read access to)
2. WriteView(Specifies SNMP view the group has write access to)
3. NotifyView(Specifies SNMP view the group will receive notifications for)

It is possible to configure a group with read access to one SNMP view, and write access to a different SNMP view.

Note: *The Allied Telesyn implementation of SNMPv3 does not support "Context Names", and will ignore the context name field in any incoming SNMPv3 packets.*

SNMP Groups

An SNMP group is essentially an access control policy to which users can be added. Each SNMP group is configured with a security level, and is associated with an SNMP view. These parameters specify what type of authentication and privacy a user within the SNMP group will use, and also what objects in the MIB the user can access. Each SNMP group name and security level pair must be unique within a switch or router.

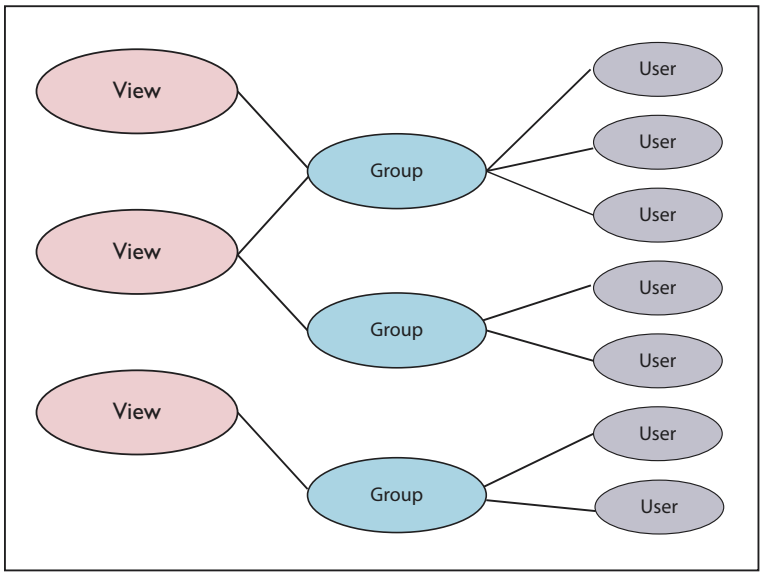
SNMP Users

SNMP users have a specified username, authentication password, privacy password, (if required) and authentication and privacy algorithms to use. The authentication algorithm options are none, MD5, or SHA. The privacy algorithm options are none, or DES. When a user is created, it is associated with an SNMP group.

Note: *It should be noted that the concept of SNMP communities that was introduced in SNMPv2 is not relevant to SNMPv3, and has been replaced by SNMP groups/users. However it is possible to configure an Allied Telesyn device to respond to both SNMPv2 and SNMPv3 requests. In this instance you would configure SNMP communities and SNMP groups/users.*

Relationship between users, groups and views

You can create multiple views on a switch or router. You can then create multiple groups and associate them with a view. It is possible to have more than one group (with a different name and security level) associated with a particular view. It is also possible to have more than one view associated with a group. (e.g. - A group could have read access to the whole MIB tree, but only have write access to certain objects.) You can then create multiple users and associate them with a group. It is possible to have many users associated with a particular group. (see diagram below)



Targets

SNMPv3 also introduces the concept of targets. An SNMP target is essentially an IP address where SNMP notifications and traps are sent. There are two parts to an SNMP target:

SNMP Target Address

An SNMP target address specifies the destination and user that receives outgoing notifications, such as trap messages. SNMP target address names must be unique within the managed device.

SNMP Target Params

An entry in the target-params table can be used to apply a security profile to one or more management targets, and is used in conjunction with the ADD SNMP TARGETADDRESS command to specify the security profile for a target address. SNMP target params names must be unique within the managed device.

Configuration example

Below is a typical example of a customer SNMPv3 configuration: (The hashed comment above each line explains the function of that CLI command.

#Enables SNMP

```
enable snmp
```

#Enables SNMP authentication failure traps.

```
enable snmp authenticate_trap
```

#Adds SNMP target parameters set, to specify a security profile for target addresses.

```
add snmp targetparams=netmonpc securitylevel=authpriv user=steve
```

#Adds a target address where traps will be sent.

```
add snmp targetaddress=nms ip=192.168.11.23 udp=162 params=netmonpc
```

#Creates an SNMP view which will allow access to everything from the specified Object Identifier (OID) onwards.

```
add snmp view=full oid=1.3.6.1 type=include
```

#Creates an SNMP view which will allow access to everything from the specified OID onwards, and also adds a restriction to anything on a particular sub-tree.

```
add snmp view=restricted oid=1.3.6.1 type=include
add snmp view=restricted oid=1.3.6.1.6 type=exclude
```

#Adds another restriction to SNMP view "restricted", preventing access to the specified MIB name and everything below it. This is an alternative to the command syntax shown in the command above, and it should be noted that commands entered with the syntax shown below will appear in the configuration with the syntax above - i.e. as an OID.

```
add snmp view=restricted mib=bgp type=exclude
```

#Creates an SNMP group which has full read/write and notify privilege to the ‘full’ view, and specifies authentication and privacy.

```
add snmp group=super-users securitylevel=authPriv readview=full
  writeview=full notifyview=full
```

#Creates an SNMP group with full read and notify privilege to the ‘full’ view, and specifies authentication but not privacy.

```
add snmp group=users securitylevel=authnoPriv readview=full
  notifyview=full
```

#Creates an SNMP group with read access to the ‘restricted’ view only, with no authentication or privacy specified.

```
add snmp group=restricted-users securitylevel=noAuthNoPriv
  readview=restricted
```

#Creates an SNMP user and associates it with the ‘super-users’ group, and specifies the authentication and privacy protocol and the authentication and privacy passwords.

```
add snmp user=steve group=super-users authprotocol=MD5
  authpassword=cottonsox privprotool=DES privpassword=woollytop
```

#Creates an SNMP user and associates it with the users group, and specifies the authentication protocol and password.

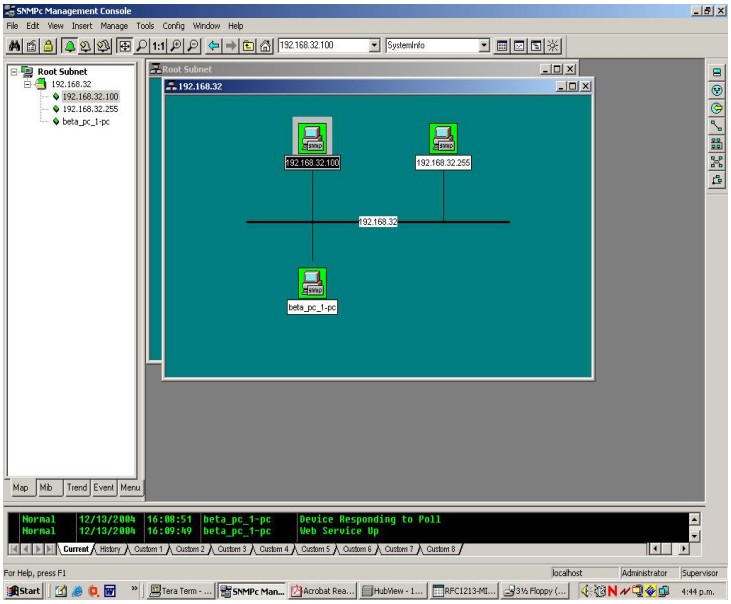
```
add snmp user=mike group=users authprotocol=MD5 authpassword=redjeans
```

#Creates an SNMP user and associates it with the restricted-users group. Note: No authprotocol or authpassword are specified for this user as the group restricted-users has a security level of ‘NoAuthNoPriv’ (i.e. no security)

```
add snmp user=paul group=restricted-users
```

CastleRock SNMPc

The following captures show what you would need to configure in SNMPc to communicate with an Allied Telesyn device.



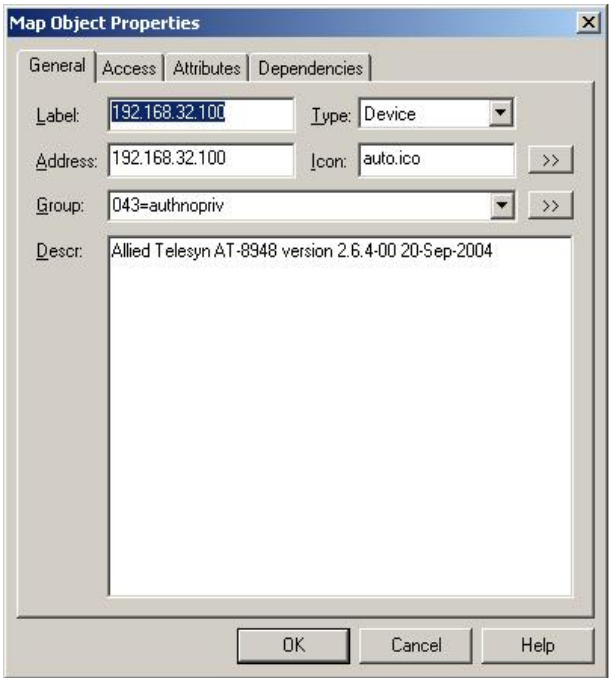
This is the main console window.

1. Right click on an object in the Map window, then select **Properties**.

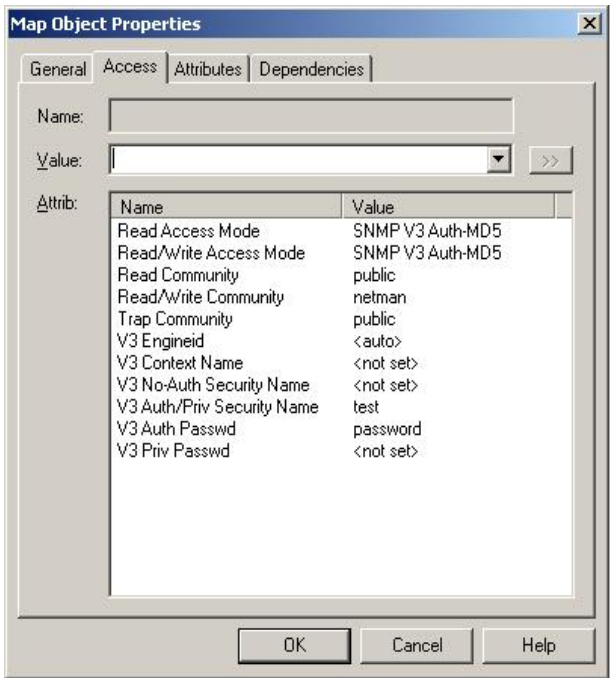
   The Map Object Properties window opens.

2. Click on the **General** tab.

   This is where you configure the IP address of the SNMP device that the Map object refers to.



3. Click on the **Access** tab. This is where you can configure SNMPv2 read and write community for this Map object. This is also where you configure any SNMPv3 parameters for this Map object.



USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesyn.com

C613-16060-00 REV A