SNMP inventory

Inventory of SNMP systems

TITLE	SNMP inventory
AUTHOR	Docusnap Consulting
DATE	10/10/2023
VERSION	3.1 | valid from October 6, 2023

CONTENTS

1. Introduction

Active network components such as switches, routers, and printers can be captured using SNMP inventory with Docusnap.

SNMP inventory in Docusnap supports versions v1, v2c and v3, querying various predefined Management Information Bases (MIB), such as the Printer MIB or the RFC1213 MIB.

The collected data can then be presented in the form of reports (text form) or maps (graphical presentations such as topology and VLAN maps).

You can use SNMP inventory for the following purposes:

- Inventory and documentation of network components
- Evaluation which systems can be found at which switch, port and VLAN

2. Requirements

2.1 General Requirements

To perform a successful SNMP inventory of a system, the following requirements must be met.

- SNMP v1, v2c or v3 must be enabled.
  - For v1 or v2c a read community string must be used
  - For v3, appropriate authentication data must be used
- The SNMP systems must be reachable from the Docusnap server / discovery service system (firewall?)
- A complete representation of the topology requires the following protocols on switches, routers and firewalls:
  - Cisco Discovery Protocol (CDP)
  - Link Layer Discovery Protocol (LLDP)

If, despite the above requirements, not all systems can be inventoried, the following must be checked:

- Are the requests blocked by monitoring, firewall or other security solutions?
  - Flooding Protection (ICMP, UDP)
  - Intrusion Protection
- Check IP address based access lists
  - Which IP addresses are allowed to access the systems via SNMP?
- Correctness of the community string, or the SNMPv3 authentication data?
- Up-to-dateness of the firmware of the SNMP systems?
- In case of missing topology information or no connections in the topology map, check the activation of the neighbor protocols via CLI or web (LLDP, CDP).
  - E.g. show lldp neighbors / show lldp interface

The names of the inventoried SNMP systems are derived from the system name of the devices if this is maintained and present on the systems (OID: 1.3.6.1.2.1.1.5).

Alternatively, it can be activated in the inventory options that not the system name, but the DNS name is used.

If the system name is not maintained, the IP address is used as the name. For this reason, it is recommended to maintain the system names of the SNMP systems accordingly, since the display with the IP address or also the standard SNMP names of the systems may not be very meaningful.

We recommend using the system name instead of the DNS name.

2.2 Requirements CISCO SNMPv3

For Cisco devices, additional requirements are required if they are inventoried via SNMPv3. If these requirements are not met, the **learned MAC addresses** and **VLAN assignments** may not be read out. This in turn affects the correct display of the topology- and VLAN-map.

You will find the corresponding information on the following pages:

- https://community.cisco.com/t5/network-management/vlan-bridge-mib-and-snmpv3-contexts/td-p/1589698
- https://www.netnea.com/cms/2015/01/09/netdisco-with-snmp-v3-and-cisco/
- https://community.cisco.com/t5/network-management/bridge-mib-with-snmp-v3/td-p/1179194

We do not assume any liability for the correctness of the contents of the previously linked websites.

3. SNMP Inventory

Docusnap supports SNMP version v1, v2c and v3. v1 and v2c versions are combined in one step in the SNMP Inventory Wizard, v3 is configured in another step.

For SNMP inventory start the corresponding wizard:

- Discovery - All Wizards - SNMP
- Inventory - All Wizards - SNMP
- All Jobs - All Wizards - SNMP

In **step 1**, select your company or your customer's company.

In **step 2**, select the discovery service through which you want to perform the inventory.

For a scheduled inventory, select the Docusnap Server Discovery or a discovery service configured by you here.

Furthermore, select or specify a / the domain below which the systems to be inventoried are to be sorted.

3.1 SNMP V1 / V2

In **step 3**, ALL IP address ranges that you have in use are now required.

Further you deposit the reading community.

If there are devices with different community strings in the IP range, you can enter the community strings in comma-separated form

You can also prepare and import the IP address ranges in a CSV file. The following structure is assumed:

IP from	IP to	Community	Timeout
192.168.0.1	192.168.255.255	public, MyCommunity	2500
10.0.0.1	10.0.0.255	public, MyCommunity	2500

It is not recommended to make any change to the following settings:

- Inventory device data for individual v1 and v2 systems (Active).
- Inventory topology information for v1 and v2 systems (Active)
- Reduce inventory to minimum amount of data (Inactive)

Limit pings executed Parallel during the inventory to

- Reduce this value if you individual systems are not inventoried during the inventory process or your monitor / security solution alerts.

Check system availability via ping

- In the first step the SNMP systems are pinged - if no ping is possible, no inventory takes place
- If the ping is deactivated for security reasons, deactivate this option as well.

Furthermore, the timeout settings should be observed if Cisco devices are in use. If you cannot reach all systems here, it is recommended to increase the timeout. This is necessary because Cisco devices sometimes respond to requests later.

3.2 SNMP V3

In **step 4** you store the SNMPv3 systems to be inventoried via the button +New.

You can store a specific system or IP range.

The corresponding SNMPv3 login data must then be entered.

The login data can also be taken over from an already stored system.

Take over login data for all systems

In this case the stored credentials are applied to all existing and future SNMPv3 systems.

If you have a large number of SNMPv3 systems / IP ranges, it is advisable to import them by loading a list. In this CSV file, not only the host name or the IP address can be transferred, but also the necessary login data. The CSV file must have the following structure - for the import remove the line with the headers!

Name / IP	User	Auth Alg.	Auth. Pwd.	Privacy Alg.	Privacy Pwd.	Context	Timeout
192.168.100.1-192.168.100.100	Docusnap	SHA384	Password	AES256	Password	Kontext	2600
192.168.101.1-192.168.101.100							
192.168.100.101	Docusnap	SHA512	Password	AES128	Password	Kontext	2600
192.168.100.102	Docusnap	SHA256	Password	AES	Password	Kontext	2600

If the systems have the same credentials, it is sufficient to enter them for the first system.

If the security level **Auth_NoPriv** is selected, then leave the fields for **Privacy Algorithm and Privacy Password** empty. You can also leave the **context** name blank if none has been configured.

Even with SNMPv3, it is not recommended to make any changes to the following settings:

- Inventory device data for individual v1 and v2 systems (Active).
- Inventory topology information for v1 and v2 systems (Active)
- Reduce inventory to minimum amount of data (Inactive)

4. Analysis

4.1 SNMP Systems

The inventoried data of the SNMP systems can be viewed as usual via the tree structure

- Your company - Infrastructure - Your domain - SNMP systems

The inventoried SNMP systems are now listed according to their device type. How to adjust and extend these assignments is described in chapter Assign SNMP types automatically / Assign SNMP types manually.

4.2 Topology map

Docusnap can inventory the topology of corresponding network devices (switches, routers, etc.). This means that the direct connections of network devices are read and displayed in the topology map.

In addition, a port allocation map of switches is created based on the learned MAC addresses and displayed in the topology map. This information can be found in the detailed map of a switch.

The detail map of a switch resolves the learned MAC addresses of the switch, provided that the corresponding device has been inventoried and is thus known in Docusnap. If the device is not yet known, only a MAC address and the manufacturer are displayed at the port - this is done using the manufacturer part of the MAC address. IT assets and manually created systems that you have documented with network information (especially the MAC address) are also displayed in the topology map.

It is important to note that the Topology map only uses the data from the last inventory. Furthermore, the learned MAC addresses of the switches are volatile. This means that ports forget learned MAC addresses again if the connected systems are inactive for a longer period of time. Therefore the inventory of SNMP systems, especially the switches, should be done at "peak times".

The following is a list of which systems etc. are listed in the topology map

- SNMP devices of switch type
- SNMP devices with topology information (CDP, LLDP) - e.g. access points
- IP systems and MAC addresses detected by LLDP and CDP information from switches
- Generally devices which are redundantly plugged on more than one switch
- Router

The topology map can be created and exported ad-hoc, via the tree structure. In addition, the map can also be exported automatically and time-controlled (PNG, HTML, VDX, SVG).

Via the tree structure you can find the topology map at the following locations and in the following versions:

Your company - Infrastructure - Standard maps - Topology map.

- Company-wide devices are used for the topology map - cross-domain.

Your company - Infrastructure - Your domain - Standard maps - Topology map

- Only the devices of the domain are used.

Your company - Assets - System groups - Your domain - System group - Standard maps - Topology map

- Only the devices of the selected system group will be used.

Your company - Locations - Location - Documentation - Topology map

- Only the devices of the selected and the subordinate sites are consulted.

Your company - Infrastructure - Your domain - Systems (Server, Linux,...) - Documentation - Topology map

- It is shown in a simple graphical representation to which switch and port the selected system is connected.

Your company - Infrastructure - Your domain - SNMP systems - Switch - Documentation - Topology map

- The detailed map of this switch is displayed

Your company - Infrastructure - Your domain - System (Windows, Linux, Mac etc.) - Documentation - Topology map

- Topology of the system - switches to which the system is connected

4.2.1 Topology map - options

After you have opened the topology map, a separate area with options is available in the action menu. For example, you can export the map. Furthermore, you have the following options available, which have a direct effect on the map.

In the Docusnap options, you can also set defaults for the following settings:

- Options (title bar - gear) - Documentation - maps- Settings Topology maps and VLAN Visualization.

Special

Show potential access points

- Displays potential access points in the overview map. Potential access points are detected based on CDP or LLDP entries of the switches, but they are not present in the Docusnap database.

Show Layer 3 elements

- Layer 3 systems, e.g. routers, are displayed in the overview map.

Show tunnel connections

- If a tunnel connection is known via LLDP or CDP, this option displays the connection.

VLAN

Show VLAN tables

- This option displays the respective VLANS for switches as a table.
- VLAN tables with the same content are colored the same.

Show ports with VLAN information

- This option displays the tagged and untagged information for the ports in the detailed maps for the switches.

Filter on relevant VLANs

- Only relevant VLANs are displayed. VLANs that are active on switches but not on any port are ignored.

Details

Show details

- Switch details, cable bandwidth and port name can be displayed.

Virtual

Hide virtual structures

- Hides the virtual switches in the overview map.

Virtual switches

- Detailed maps of the virtual switches are not created.

Visualization

Visualize cable bandwidth

- This option colors the lines of a connection differently, depending on the speed.
- If the speed is higher, a thicker line is used.
- If the speed exceeds 10 Gbit/s, the line is displayed in blue.

- If the speed falls below 1 Gbit/s, it will be displayed in red.
- In the other cases the line is drawn in green color.

Highlight missing data

- This option highlights switches where no LLDP, CDP or Spanning Tree information is available.
- Furthermore, devices are highlighted if no learned MAC addresses are available or the interface stack data is missing.
- By right-clicking on the highlighted object - Show data, the error message is displayed in an additional dialog.

4.3 VLAN Map

In the first embodiment, you will notice that the VLAN plan outputs the same information that you receive within the topology plan with the VLAN tables option.

The overview plan shows the connections of the switches to each other with the VLAN tables belonging to the switch.

In addition, you can also create a VLAN detail plan. In this detailed plan, you select a VLAN. You will then see all the switches in the VLAN. The systems plugged on the switches and in the selected VLAN are also displayed.

4.4 Reports

In addition to the topology and VLAN plan, there are also reports that you can use to analyze this information of the SNMP systems. These reports can be found as follows:

- Your Company - Infrastructure - Your Domain - Reports - Infrastructure Network.

Network Devices

- The report lists all SNMP systems, with the information inventoried in the standard - including.
- General information, network information, interfaces

Printers

- All printers with the printer specific information
- Printer information, toner

Switches

- This report gives you detailed information about the switches - including
- VLAN information and their port assignment
- Listing of the ports and the systems plugged there

VLAN

- When creating the report, you can first select one or more VLANs.
- Then, grouped by the selected VLANs, you will get a list of all associated systems.

VLAN Overview Switch

- Here, too, you first select one or more VLANs
- Then you will be grouped again by the selected VLANs
- In addition, the list is now also grouped by switches on which the associated systems are plugged in - with details of the system type, MAC and IP address and port

4.5 Topology List

- Your company - Infrastructure - Your domain - Summary - Topology

This view gives you information regarding the used switch ports. For example, it can be filtered by a MAC address or system name to quickly find out which switch port the device is connected to.

If a port is listed that only shows a Mac address but not a connected system, then the system with that Mac address is not yet inventoried in Docusnap. With the filter expression \null in the Connected system column, you can filter for all unknown systems.

IT assets and manually created systems that you have documented with network information (especially the MAC address) will also be listed.

4.6 VLAN Overview

- Your company - Infrastructure - VLAN overview - VLAN total overview

In this view you can list the VLANs used and the systems within them

5. Adjustments

5.1 Edit switch - configure manual connections

It was described before that the data from the switch detail plan is provided by reading the learned MAC addresses and that these are volatile again. For complete documentation, you can also manually assign a MAC address to the switch port and document it permanently. These manually performed adjustments remain even after a new inventory!

The manual assignment takes place in the Docusnap Administration:

- Administration - Inventory - SNMP - Edit Switch.
- Select the company, the domain and then the switch
- Now select the port to be adjusted and add the MAC address

5.2 Mac Filter

It happens that some systems cannot be inventoried correctly / completely. As a result, only the MAC addresses can be found in the topology detail plan. An example for this are IP phones.

With the help of the Mac filter you can now store a part of the Mac address that matches for the devices and select whether they should be shown as a device, as a phone or not in the topology plan. You can store the Mac addresses in the Docusnap Administration.

- Administration - Inventory - SNMP - Mac Filter

Enter an appropriate MAC filter - * can be used as a placeholder.

6. Type SNMP devices

The SNMP systems are displayed in the tree structure grouped by their type. It is possible that no assignment has taken place (type General) or that you want to adjust an existing assignment.

Mapping the devices to your type increases the quality of the data that is in Docusnap. You can find out much faster this way how many printers, switches, routers, UPS, webcams, etc. are in use. SNMP systems are also displayed with meaningful icons in the available plans.

The assignment can take place automatically, on the basis of search words, or manually.

The predefined SNMP types can be extended by own types.

6.1 Assign SNMP types automatically

The automatic assignment takes place on the basis of defined keywords within the device description of an SNMP system. The description field can be found as follows:

- Your Company - Infrastructure - Your Domain - SNMP Systems - SNMP System Type
  - SNMP System - Inventory Date - General - Description

Now, if you want to assign an unassigned system, find one or more related words from the description field - e.g.

Description	Keyword
HPE StoreOnce 2700 Backup	%Backup%
HP ETHERNET MULTI-ENVIRONMENT,ROM none,JETDIRECT,JD149	%JETDIRECT%
HP Onboard Administrator	HP Onboard Administrator
Integrated Lights-Out 4 2.62 Jan 09 2019	%Integrated Lights-Out%
HP P2000 G3 FC	%P2000%
HPE_3PAR 7200, ID: 53216, Serial number....	%3PAR%
HP J4813A ProCurve Switch 2524, revision F.05.80, ROM F.02.01	%ProCurve% oder %Switch%

The new keywords are stored in Docusnap Administration

- Administration - Inventory - SNMP - SNMP Types
  - New
    Enter the keyword and select the appropriate type
    %.....% serves as a placeholder

6.2 Assign SNMP types manually

Manual assignment may be necessary if an SNMP system does not provide a description or this cannot be used for a unique assignment.

A manual assignment is not overwritten using keywords!

The manual assignment can be done in the data area or in the context menu.

Data area

In the data area, several devices can be assigned to an SNMP type using the checkboxes. After selecting the devices, you can assign them to an SNMP type. You can also remove the manual assignment.

The column Fixed SNMP Type gives information whether this device was assigned to the SNMP type by an automatism, or by manual assignment.

Context menu

From the context menu (right click on the system in the tree structure) a specific system can be manually assigned to an SNMP type.

6.3 Define own SNMP types

You also have the possibility to create your own SNMP types - in case the predefined SNMP types are not sufficient.

Own SNMP types are created and managed in the administration:

- Administration - Inventory - SNMP - SNMP Basic Types.
- New
  - *Name*
  - *Value* - recommendation: starting from 1000
  - *Text German*
  - *Text English*

You can also add suitable icons to these own SNMP types.

- Administration - Customizing - Icons - Icons
- New
  - *Group* - SNMP
  - *Value* - value of the previously created SNMP type
    Can also be selected by reference value
  - *Standard icon* - 16x16, png format
  - *Preview icon* - 100x100, png format

The Docusnap Icon Pack is available for download in our Community, in the Benefits, Customizing - Docusnap Icon Pack section.

7. Manufacturer-specific MIBs

The SNMP inventory can be extended by the integration of manufacturer-specific MIBs. This allows additional OIDs to be read out during the inventory. It should be noted that this additional information must be prepared accordingly (view, report), since it is only visible in the SNMP explorer.

Manufacturer-specific MIBs can ensure that far more information is inventoried. For this reason, including them can increase the inventory time many times over.

It is not recommended to import vendor-specific MIBs "just because". The correct approach is:

- Get an overview of what information is useful with the vendor-specific MIBs.
  - Preferably via manufacturer information of the SNMP devices
- Under which OIDs this information can be found
- Import the MIB
  - Assign the MIB to the SNMP system type
  - Activate only the relevant OIDs

7.1 Include manufacturer specific MIB

Vendor specific MIBs are imported in the Administration of Docusnap:

- Administration - Inventory - SNMP - SNMP MIBs - Import.

IMPORTANT!

MIBs have dependencies on other MIBs. When you import a MIB, you may get an error message if the dependency could not be resolved.

In this case, collect the MIBs specified in the message in a folder and then run the import again.

After the successful import, select the associated SNMP system type in the next step. This indicates that the MIB should be executed on UPS or firewalls, for example.

In the next step, you can customize the information to be inventoried in the Browse MIBs section. For example, it is always recommended to deselect TRAPS. Since querying these can cause problems on some systems.

7.2 Evaluate data

The additional information read out by the MIB import can first be found in the SNMP Explorer.

- Your Company - Infrastructure - Your Domain - SNMP Systems - SNMP System Type
  - SNMP system - inventory date - SNMP Explorer - SNMPv2-SMI
    - org - dod - internet - private - enterprises

This is followed by the structure of the imported MIB. E.g. for the Sophos MIB

- sophos - xg-firewall - sfosSystem - sysInstall – applianceModel
  OID: 1.3.6.1.4.1.21067.2.1.1.2.0

This information can also be listed in a view, or in a new node in the tree structure.

In the first step, the corresponding OIDs are required for this - e.g. the following, from the Sophos MIB

- 1.3.6.1.4.1.21067.2.1.1.0 - ApplianceKey
- 1.3.6.1.4.1.21067.2.1.2.0 - ApplianceModel
- 1.3.6.1.4.1.21067.2.1.1.3.0 - xg-firewallVersion - is called firmware

The second step is to create a new view in Docusnap Administration:

- Administration - Customizing - Manage Tables
- +New
  - *Table type* - view
  - *Table name* - xv - SophosMib - SophosMibView
    - xv is predefined by Docusnap
    - *SophosMib* is the name of the namespace for customizing
    - *SophosMibView* is the actual name of the view
      The view is then called *xvSophosMIBSophosMibView*
- *German Name*
- *English Name*
- *SQL Statement*[1]
  SNMP-Single:
  (1.3.6.1.4.1.21067.2.1.1.1.0,ApplianceKey;1.3.6.1.4.1.21067.2.1.1.2.0,ApplianceModel;1.3.6.1.4.1.21067.2.1.1.3.0,Firmware)

The next step is to create the fields of the view - Edit fields:

Field Name	Data Type	German name	English Name
ApplianceKey	String	Appliance Key	Appliance Key
ApplianceModel	String	Appliance Modell	Appliance Model
Firmware	String	Firmware	Firmware
ValueID	BigInt	ValueID	ValueID

The ValueID serves as the primary key. For this field you can deactivate the option Show field in lists.

[1] To output values that occur only once for each SNMP device, e.g. the serial number, the statement is started with SNMP-Single. If a table is output, then the statement is started with SNMP. For example, the IP addresses of a system.

Now select the primary key and the display field.

Now the new view will be integrated into the data tree.

- Administration - Customizing - Manage objects

Select in the object hierarchy:

- Account - NetworkEnvironment - Domain - SNMP Systems
  - SNMPTypes_Data - SNMP_Data - SNMPDocu_Data

Create two new objects - +New

Object name	Category	Namespace	German name	English name	Default Icon	Preview Icon
SophosMibView	Überschrift	SophosMIB	SophosMibView	SophosMibView	16x16, png	100x100, png

Object name	Category	Table	German name	English name	Icons
SophosMibView_Data	Daten	xvSophosMIBSophosMibView	SophosMibView_Data	SophosMibView_Data	Siehe oben

Now the data is displayed in the tree structure.

For more information on creating and integrating views, see HowTo: Customizing - Creating a data view in the Knowldge Base.

8. SNMP troubleshooting - Checklists

Often the same errors occur with the SNMP inventory. To provide you with an opportunity for quick analysis and troubleshooting outside the classical support, two checklists are available for SNMP inventory. Docusnap Support first checks the same points for SNMP problems.

The first checklist deals with the solution of the SNMP inventory itself. The second checklist covers troubleshooting for missing topology information.

The checklists speak of SNMP agents and SNMP managers. These two terms essentially describe the function of the respective system.

SNMP Manager

Query system, e.g. Docusnap Server or Docusnap Client.

SNMP Agent

The queried system (to be inventoried). E.g. printer, switch, router, or other SNMP capable network devices.

8.1 Checklist - SNMP inventory not possible

1. ☐ Supports SNMP target system
    a. ☐ Yes: continue with next step
    b. ☐ No: SNMP inventory is not possible. Device must be recorded manually
2. ☐ Is the SNMP protocol enabled on the agent?
    a. ☐ Yes: continue with next step
    b. ☐ No: Activate SNMP
3. ☐ Is communication via ping between SNMP agent and manager possible?
    a. ☐ Yes: continue with next step
    b. ☐ No: Check network connection or do not check system availability during SNMPv1/v2c scan
4. ☐ Does the communication between SNMP agent and manager take place via an additional network device, e.g. a firewall?
    a. ☐ No: continue with next step
    b. ☐ Yes: Check firewall log. If necessary, this blocks the connection.
5. ☐ Which SNMP version is supported?
    a. ☐ SNMP v1/ v2
        i. ☐ Is the correct community string used?
            1. ☐ Yes: continue with next step
            2. ☐ No: Customize Community String
    b. ☐ SNMP v3
        i. ☐ Authentication data correct?
            1. ☐ Yes: continue with next step
            2. ☐ No: Adapt authentication data
6. ☐ Check if there is a Backslash or an @ in the Community String / Username / Password
    a. ☐ No: continue with next step
    b. ☐ Yes: Change password. Many systems have a problem with special characters
7. ☐ Is the SNMP Manager (querying system, Docusnap client or server) authorized for SNMP queries?
    a. ☐ No: Authorize SNMP Manager to SNMP Agent for SNMP Polling.
    b. ☐ Yes
        i. ☐ Is the right SNMP manager querying the right system?
            1. ☐ Yes: continue with next step
            2. ☐ No: Select the correct SNMP manager-system
8. ☐ Does the configured access have to be authorized to the OID tree?
    a. ☐ Yes: continue with next step
    b. ☐ No: Assign permissions to the community or group.
9. ☐ If the query is blocked by (monitoring) firewalls or security solutions (flooding protection, intrusion protection), if necessary
    a. ☐ No: continue with next step
    b. ☐ Yes: configure appropriate exceptions
10. ☐ Check if Docusnap can perform an inventory.
    a. ☐ Yes: Checklist successfully completed
    b. ☐ No: check if SNMP Agent is part of the configured IP segment
        i. ☐ Yes: continue with next step
        ii. ☐ No: Add IP segment
11. ☐ Check if 3rd party tools, like the Paessler SNMP Tester, can read the data (Description, Interfaces)
    a. ☐ No: continue with next step
    b. ☐ Yes: Contact Docusnap Support

12. ☐ Is the firmware of the SNMP agent up to date?
    a. ☐ Yes: continue with next step
    b. ☐ No: Check update for current version. (no warranty on the part of Docusnap Support)
13. ☐ Contact Docusnap Support

8.2 Checklist – missing topology information

LLDP

Link Layer Discovery Protocol

CDP

Cisco Discovery Protocol

1. ☐ Supports SNMP system neighborhood protocols (CDP, LLDP)
    a. ☐ Yes: continue with next step
    b. ☐ No: Topology only possible via manual configuration
2. ☐ Is LLDP or CDP activated?
    a. ☐ Yes: continue with next step
    b. ☐ No: Activate LLDP or CDP
3. ☐ Is a uniform neighbourhood protocol used?
    a. ☐ Yes: continue with next step
    b. ☐ No: Configure uniform neighborhood protocol
4. ☐ Does the configured access still have to be authorized on the OID tree?
    a. ☐ No: continue with next step
    b. ☐ Yes: Assign permissions to the community or group.
5. ☐ Is the firmware up to date?
    a. ☐ Yes: continue with next step
    b. ☐ No: Check update for current version. (no warranty on the part of Docusnap Support)
6. ☐ Contact Docusnap Support

VERSION HISTORY

Date	Description
April 16, 2019	Version 1.0 created
September 27, 2019	Description Topology Map and VLAN Map adapted and extended
December 19, 2019	Added checklist for SNMP troubleshooting and SNMP inventory with Docusnap
May 06,2020	Version 2.0 - Revision of the HowTos for Docusnap 11
June 3, 2022	Created Chapter 5.2 - Define own SNMP types
January 04, 2023	Version 3.0 – Revision of the HowTo for Docusnap 12
October 06, 2023	Version 3.1 - Comma separated input of community strings / Use SNMPv3 IP ranges