VOSS Insights
DS9 for NetFlow Install Guide

Release 22.1

Jun 02, 2022

Legal Information

Please take careful note of the following legal notices:

-
- VOSS, VisionOSS and VOSS Automate are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

DOCUMENT ID: 20220602124604

Contents

1. VOSS Insights DS9 for NetFlow Base Environment Installation

1.1. VOSS Insights DS9 Standalone Installation

VOSS Insights DS9 is a standalone single server to collect, process and store NetFlow-v5/v9/v10 and SNMP data. Visualization of the data will be handled via the VOSS Insights Dashboard reporting.

1.1.1. Assumptions

- Host machines will be located within the same sub-network
- All the required TCP/UDP ports are open between DS9, Dashboard and NetFlow sources.
  - TCP: 5432 - 8082
  - UDP Depending on desired vflow: 2055 - 9996 - 4739 There is no redundancy requirement for any of the components
- Internet access is available to the DS9 system during installation.

  After the installation, no internet access is necessary.
- Customer premises equipment is sending NetFlow data to Collector successfully Collector can access customer premises equipment via SNMP v1/2/3 successfully

1.1.2. Installation

Items that will be needed during configuration:

1. Hostname
2. Dashboard Reporter IP
3. For each NetFlow device added:
   - IP of device
   - NetFlow version
   - SNMP version
     - v1 or v2c - community string

  - v3 - user name, user password, and encryption key
- NAT IP address (often same as IP)

2. Preparing production environment for VOSS Netflow Solution

2.1. Abstract

This document is an overview of all the action items that need to be completed by system administrators before implementation of a successful deployment.

2.2. Checklist

The following action items need to be completed by system administrators before the implementation starts:

ID	Action	Description	Criticality
1	Hardware specifications	The hardware/VM specifications have to meet the requirements defined by VOSS	Critical
2	Software specifications	VOSS Dashboard server is delivered as an ISO which includes an operating system. If this is a VM deployment, the following should be available in customer's VM datastore: • Latest ISOs. (Available at VOSS Customer Portal. Log in and select DOWNLOADS.)	Critical
3	Firewall rules	All the required traffic rules are applied to customer environment based on the firewall matrix provided by VOSS deployment Team.	Critical
4	Internet access	Internet access is enabled for the DS9 during implementation. Once the implementation is over, internet access is no longer required.	Critical
5	Round trip times (RTT)	RTT time between the DS9 and Dashboard Server is not more than 100msec.	Critical
6	Netflow configuration	Netflow sources are configured to send their Netflow data to VOSS DS9 Servers based on the suggested settings by VOSS	Critical
7	SNMP configuration	Netflow sources are configured with SNMP v1 or 2c or v3.	Critical
8	Netflow and SNMP details	Following information is provided to VOSS deployment team: • Device IP & Hostname and Netflow version for the Netflow source(s) • SNMP details for Netflow source(s)	Critical
9	Remote access	Some method of remote access is enabled for VOSS deployment team.	Critical
10	Integration to customer environment	Both DS9 and Dashboard Servers have access to customers data infrastructure for the following services: NTP, SMTP, DNS.	Critical
11	Authentication via existing customer resources	Dashboard Servers have access to customers' existing Active Directory/Identity servers to authenticate users via LDAP or SAMLv2.	Optional

2.3. Requirements

The following list of items needs to be provided to VOSS before the deployment:

ID	Action	Description	Criticality
1	IP Addresses for VOSS components	IP addresses & Subnetmasks & Default IP Gateway settings for all the VOSS Host Machines (DS9, Dashboard Servers).	Critical
2	IP Addresses for Data services	IP addresses for the following services: DNS, NTP, SMTP, LDAP/SAMLv2.	Critical
3	Remote access details	VPN access details for VOSS Team to access the DS9 and Dashboard remotely.	Critical
4	Primary and Secondary contact details	Primary and secondary contact details for technical and project management related items.	Critical
5	Email authentication for scheduled reports	SMTP authentication details for smart host servers.	Optional
6	SNMP community strings, versions and other details	SNMP community strings and protocol versions need to be provided to VOSS for successful SNMP queries.	Critical
7	List of Netflow Sources	Provide VOSS a list of Netflow sources (routers, switches) with the following details: IP addresses, Make/Model, Software Version, Netflow version.	Critical
8	List of IP addresses and Hostnames	A CSV or Excel file that maps certain IP addresses to internal hostnames can help VOSS Team to improve the data visualization experience by mapping IP address fields to hostnames.	Optional

3. DS-9 Netflow VM Sizing Specifications

VOSS Insights DS9 for NetFlow sizing specifications are divided into small, medium and large solutions based on tiers related to the number of flows that need to be supported.

Each solution below includes the VM specifications for both the VOSS Insights DS9 server and the VOSS Insights Dashboard server.

3.1. Small Netflow Solution

The three small tiers in Flows per Second:

- 1,000
- 5,000
- 10,000

Dashboard Server VM			**DS9 Netflow Collector VM**	
Cores	12		Cores	16
Memory GB	32		Memory	64
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in GB	500
			All Discs must be SSDs and Provisioned as Thick Eager Zero	

3.2. Medium Netflow Solution

Two medium tiers in Flows per Second:

- > 10,000 but <= 25,000
- > 25,000 but <= 50,000

Dashboard Server VM			**DS9 Netflow Collector** **Bare Metal Server (Dell R740 or Equivalent)**	
Cores	16		Cores	16
			CPU Needs to be Intel Gold or better.	
Memory GB	64		Memory	196
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in TB	1,5
			Read Intensive SSDs required	
			Dual Intel 10GB NIC	1
			Intel Quad 1GB NIC	1
			iDRAC Enterprise or Equivalent	
			Dual Power Supplies	

3.3. Large Netflow Solution

Two large tiers in Flows per Second:

- > 50,000 but <= 100,000
- > 100,000 but <= 200,000

Note: The DS9 Collector requires a minimum of 2 Bare Metal Servers to collect this volume in one location.

Dashboard Server VM			**DS9 Netflow Collector** **Bare Metal Server 1 (Dell R740 or Equivalent)**	
Cores	16		Cores CPU Needs to be Intel Gold or better.	16
Memory GB	64		Memory	196
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in TB	3
			Read Intensive SSDs required	
			Dual Intel 10GB NIC	1
			Intel Quad 1GB NIC	1
			iDRAC Enterprise or Equivalent Dual Power Supplies	
			Dual Power Supplies	

		Bare Metal Server 2 (Dell R740 or Equivalent)	
		Cores CPU Needs to be Intel Gold or better.	16
		Memory	196
		Disc 1 Storage in TB	3
		Disc 2 Storage in TB	3
		Disc 3 Storage in TB	3
		Read Intensive SSDs required	
		Dual Intel 10GB NIC	1
		Intel Quad 1GB NIC	1
		iDRAC Enterprise or Equivalent Dual Power Supplies	
		Dual Power Supplies	

Note:

- Larger than 200K flows per second requires special pricing and configuration.
- Distributed DS9 collection is available. This may reduce the compute required at each collection location.

4. Netflow and DS9 Monitoring System Connectivity

4.1. Communication ports between Netflow Source and DS9

Source	Destination	Protocol	Port	Direction	Description
Netflow Source	DS9	UDP	4739	Unidirectional	IPFIX (Optional)
Netflow Source	DS9	UDP	2055	Unidirectional	Netflow v9 (Optional)
Netflow Source	DS9	UDP	9996	Unidirectional	Netflow v5 (Optional)
Netflow Source	DS9	UDP	6343	Unidirectional	Sflow v5 (Optional)
DS9	Netflow Source	UDP	161	Unidirectional	SNMP queries

4.2. Communication ports between Dashboard Server Users and Dashboard Server

Source	Destination	Protocol	Port	Direction	Description
Dashboard users	**Dashboard** Server	TCP	443	Unidirectional	HTTPS (GUI access)

4.3. Communication ports between the DS9 Server and Dashboard Server

Unless the DS9 and Dashboard Servers are located in the same subnet, system administrators need to ensure the following network ports are open between these two components.

Source	Destination	Protocol	Port	Direction	Description
Dashboard Server	DS9	TCP	5432	Unidirectional	Data respository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data respository access
DS9	Dashboard Server	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

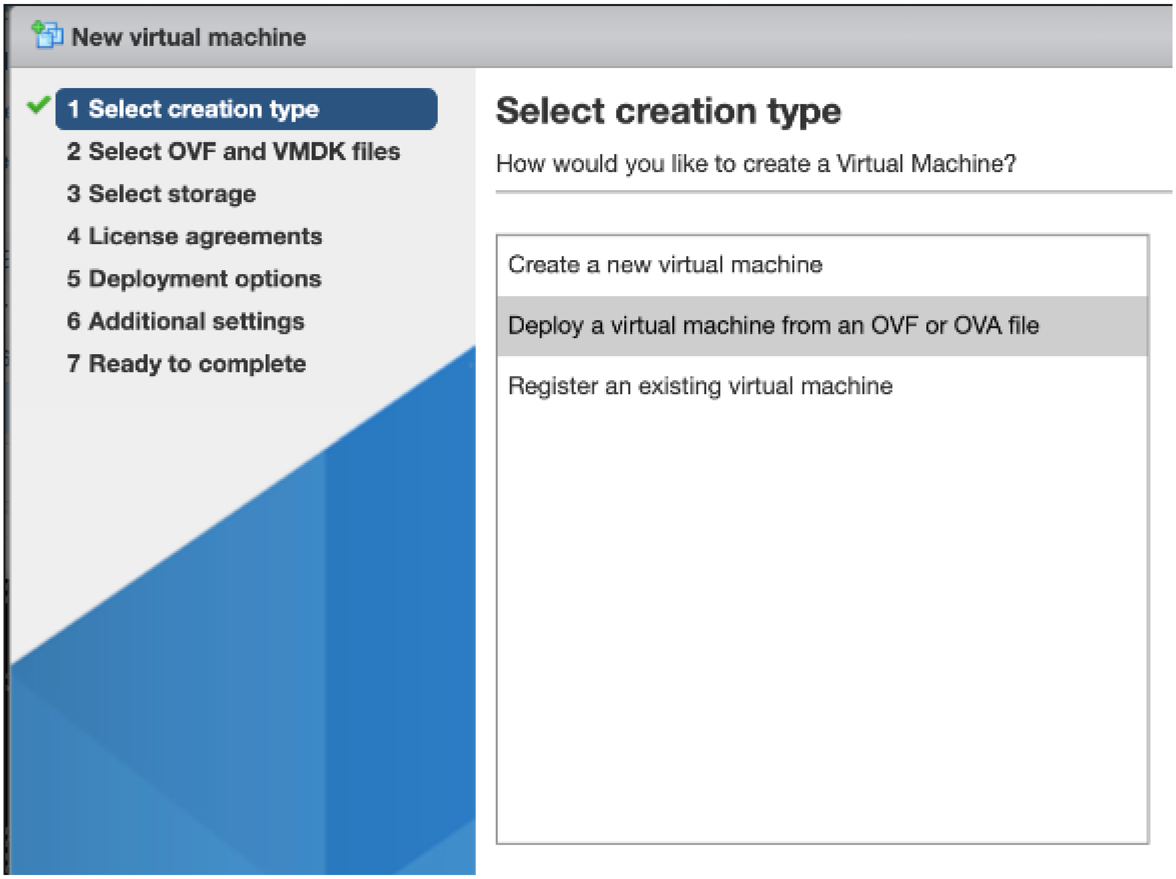
4.4. Communication ports that are required for remote management purposes

Source	Destination	Protocol	Port	Direction	Description
Admin users	DS9	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	**Dashboard** Server	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	**Dashboard** Server	TCP	443	Unidirectional	WEB access

5. Deploy and VM Installation Steps

1. Download the OVA for your system to a directory accessible by the VM client.
2. Deploy the OVA:

   Select the downloaded OVA file and choose a VM name.



New virtual machine

Select creation type

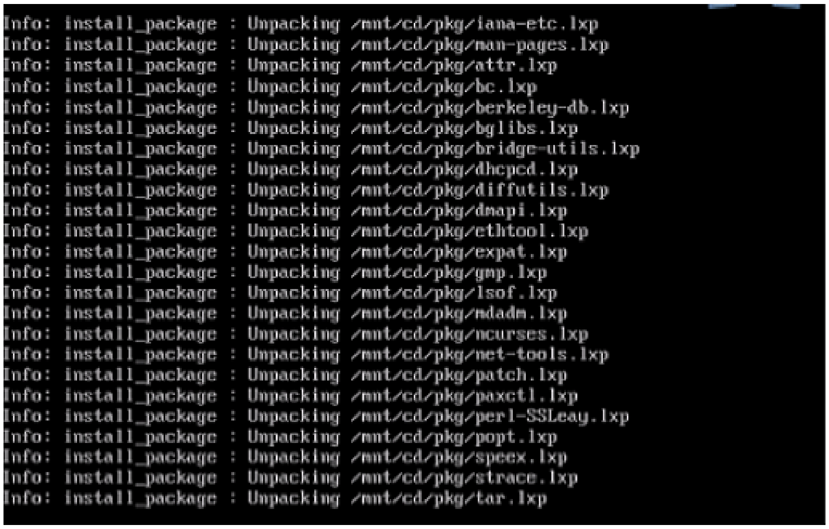
How would you like to create a Virtual Machine?

Create a new virtual machine

Deploy a virtual machine from an OVF or OVA file

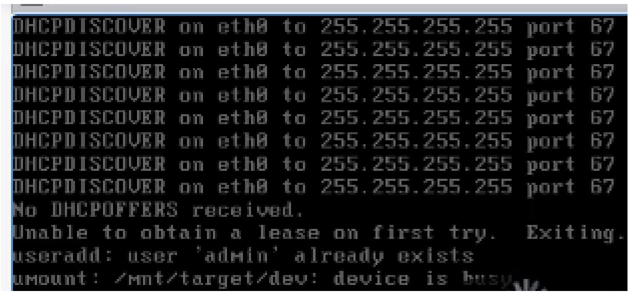
Register an existing virtual machine

3. Select *storage* according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.
4. Select *network* mappings according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.
5. When you run the VM, you will see `.lxp` packages being installed. This takes a while.



```
Info: install_package : Unpacking /mnt/cd/pkg/iana-etc.lxp
Info: install_package : Unpacking /mnt/cd/pkg/man-pages.lxp
Info: install_package : Unpacking /mnt/cd/pkg/attr.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bc.lxp
Info: install_package : Unpacking /mnt/cd/pkg/berkeley-db.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bglibs.lxp
Info: install_package : Unpacking /mnt/cd/pkg/bridge-utils.lxp
Info: install_package : Unpacking /mnt/cd/pkg/dhcpcd.lxp
Info: install_package : Unpacking /mnt/cd/pkg/diffutils.lxp
Info: install_package : Unpacking /mnt/cd/pkg/dmapi.lxp
Info: install_package : Unpacking /mnt/cd/pkg/ethtool.lxp
Info: install_package : Unpacking /mnt/cd/pkg/expat.lxp
Info: install_package : Unpacking /mnt/cd/pkg/gmp.lxp
Info: install_package : Unpacking /mnt/cd/pkg/lsof.lxp
Info: install_package : Unpacking /mnt/cd/pkg/mdadm.lxp
Info: install_package : Unpacking /mnt/cd/pkg/ncurses.lxp
Info: install_package : Unpacking /mnt/cd/pkg/net-tools.lxp
Info: install_package : Unpacking /mnt/cd/pkg/patch.lxp
Info: install_package : Unpacking /mnt/cd/pkg/paxctl.lxp
Info: install_package : Unpacking /mnt/cd/pkg/perl-SSLeay.lxp
Info: install_package : Unpacking /mnt/cd/pkg/popt.lxp
Info: install_package : Unpacking /mnt/cd/pkg/speex.lxp
Info: install_package : Unpacking /mnt/cd/pkg/strace.lxp
Info: install_package : Unpacking /mnt/cd/pkg/tar.lxp
```

6. After all the packages are installed, the VM is automatically powered off.



```
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
DHCPDISCOVER on eth0 to 255.255.255.255 port 67
No DHCPOFFERS received.
Unable to obtain a lease on first try.  Exiting.
useradd: user 'admin' already exists
umount: /mnt/target/dev: device is busy
```

You will see the `auto-poweroff` message on the console.

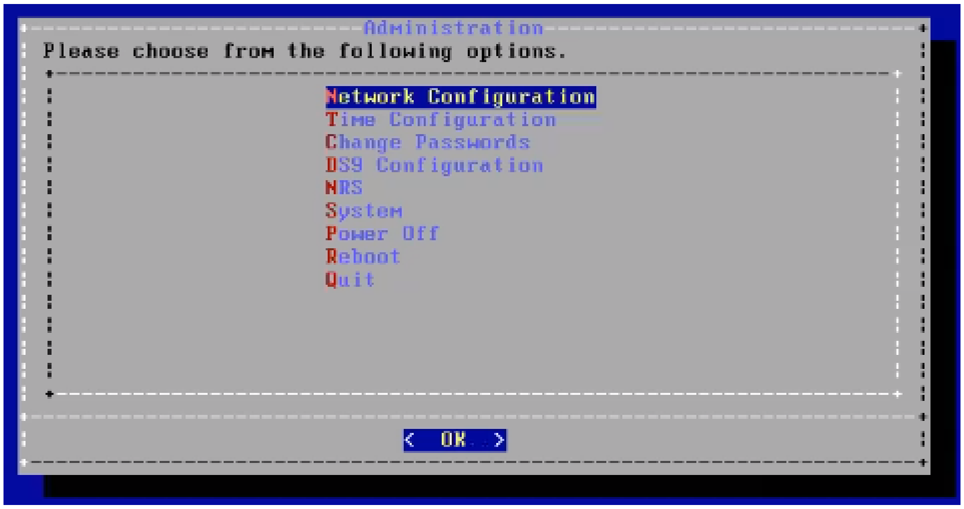
7. After the system boots, wait at the `login:` prompt until a banner with an `About` console display shows displaying values for the placeholders below:

```
                    About
==============================================
      Hostname:  <hostname>
       Version:  <version>
         Theme:  <theme>
        Flavor:
       License:  NNNNN-NNNNN-NNNNN-NNNNN-NNNNN
 Days Licensed:  nnnnn
Days Remaining:  nnnnn
   Product Key:
       Website:  <website>
        Kernel:  Linux n.nn.nn-lxt-3 x86_64 GNU/Linux

<hostname> login:
```

8. At the `login:` prompt, log in as `admin` with password as the last 10 characters of the `License:` value, *excluding the dash*.

Note: Since the Licence key value is only displayed here. When you ssh in it will not be seen. Be sure to copy out your admin password from this console.

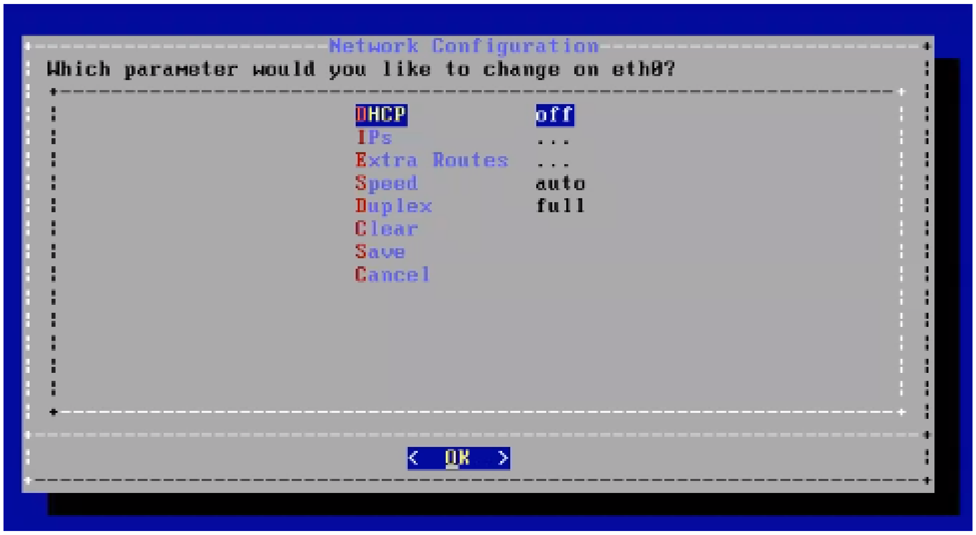
9. After login, the **Administration** menu shows, as in the example below for DS9:



```
                         Administration
 Please choose from the following options.

                     Network Configuration
                     Time Configuration
                     Change Passwords
                     DS9 Configuration
                     NRS
                     System
                     Power Off
                     Reboot
                     Quit

                          <  OK  >
```

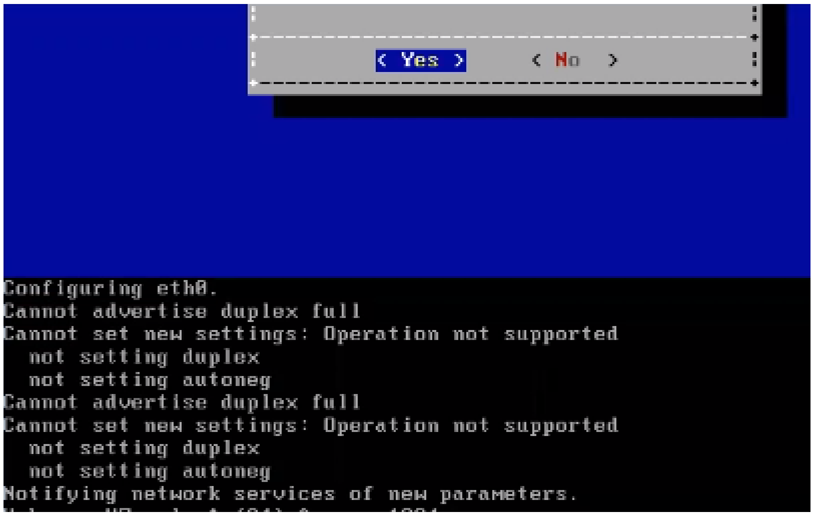
10. Under **Network Configuration**, provide ip/netmask, default gateway and hostname.

    a. Under **Interface Settings**, set the IP Address and netmask in the format, for example: `nn.nn.nn.nn/24` and save.



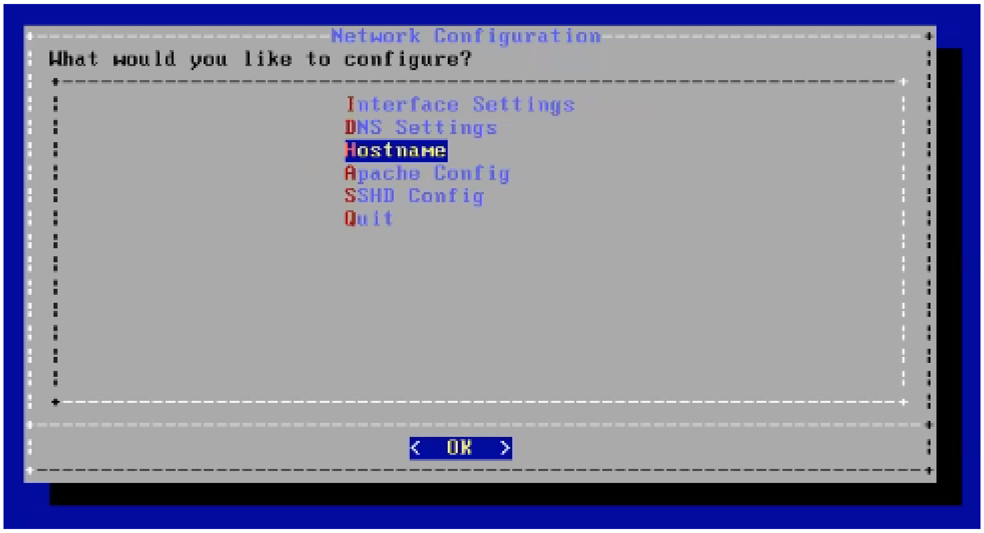
```
                    Network Configuration
 Which parameter would you like to change on eth0?

                     DHCP            off
                     IPs             ...
                     Extra Routes    ...
                     Speed           auto
                     Duplex          full
                     Clear
                     Save
                     Cancel

                          <  OK  >
```

Set up the default gateway under the **Extra Routes** menu.



```
Configuring eth0.
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Cannot advertise duplex full
Cannot set new settings: Operation not supported
  not setting duplex
  not setting autoneg
Notifying network services of new parameters.
```

b. Set hostname



The console will show the `Updating hosts:` message. Note that this setup takes a few minutes.

11. When this setup completes, you can quit the **Administration** menu on the console and continue the configuration of your system through the GUI:

    - Insights Dashboard

      See the VOSS Automate Database Setup section in the VOSS Insights Install Guide.

    - Insights Arbitrator

      See the Install Arbitrator System section in the VOSS Insights Install Guide.

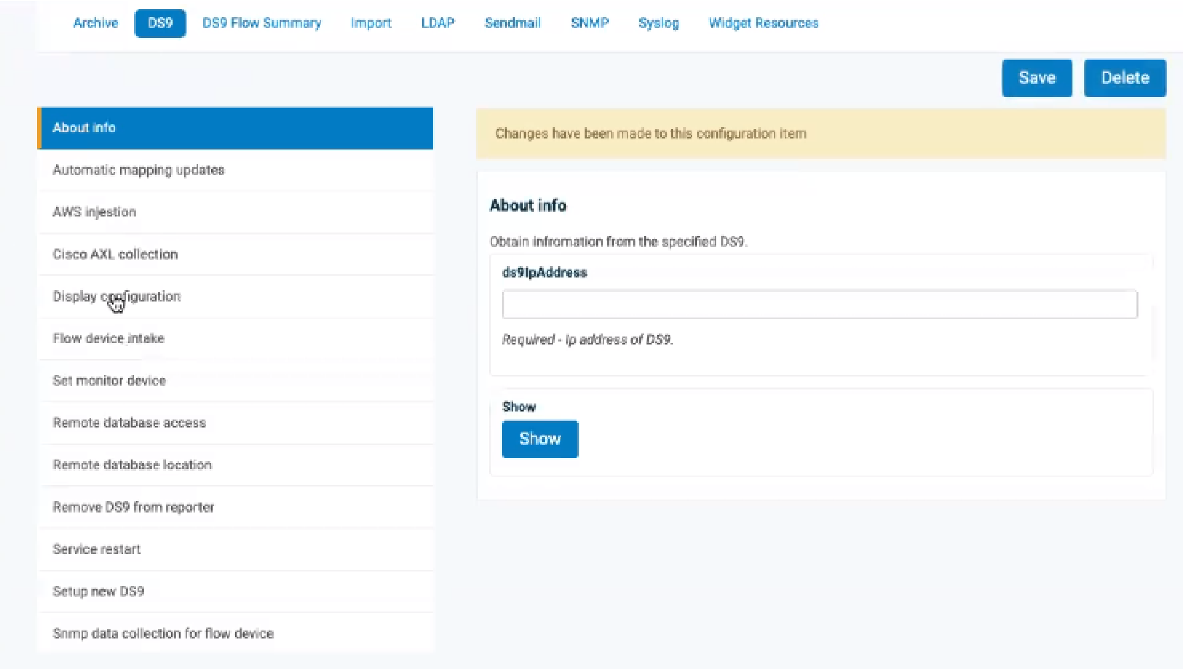
    - Insights DS9

      See the DS9 Configuration on the Dashboard section in the VOSS Insights DS9 for NetFlow Install Guide.

6. DS9 Configuration on the Dashboard

To complete the configuration between the Insights Dashboard Reporter and DS9, flow devices and SNMP configuration can be carried out:

1. Log in on the Dashboard GUI and go to **admin** > **Configuration** and on the **Configuration Settings**, go to **DS9**.



Changes have been made to this configuration item

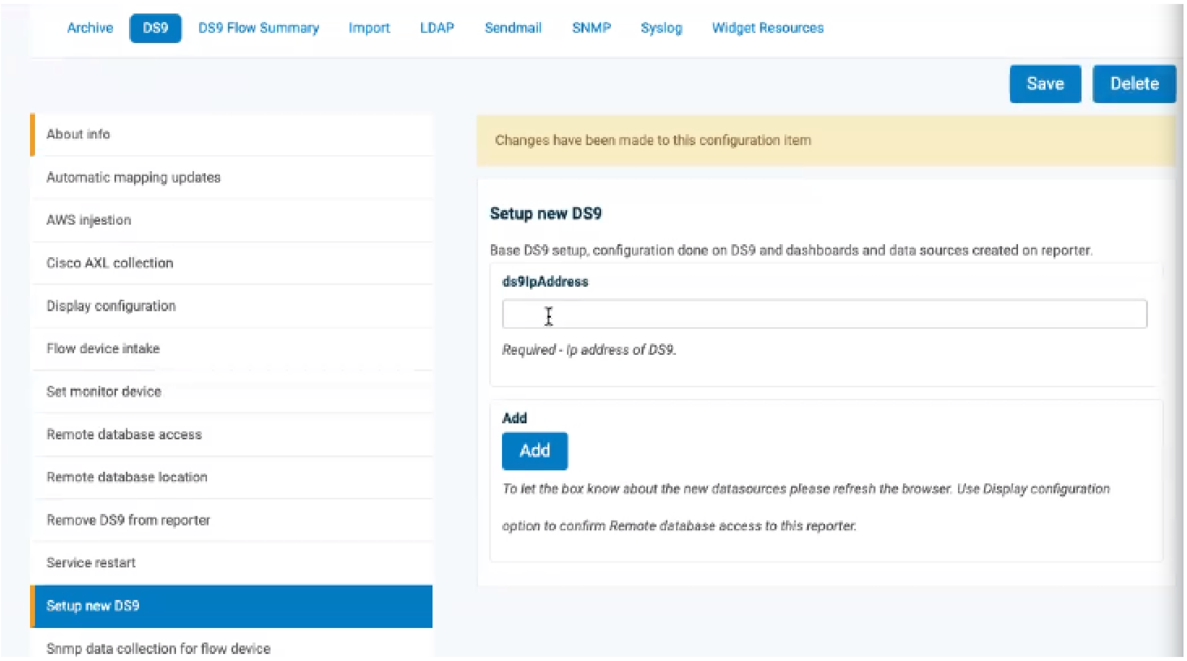
About info

Obtain infromation from the specified DS9.

ds9IpAddress

Required - Ip address of DS9.

2. Choose **Setup new DS9**, add the **ds9IpAddress** and click **Add**. Repeat this step according to the number of flow devices to set up.


Archive DS9 DS9 Flow Summary Import LDAP Sendmail SNMP Syslog Widget Resources

Save Delete

- About info
- Automatic mapping updates
- AWS injestion
- Cisco AXL collection
- Display configuration
- Flow device intake
- Set monitor device
- Remote database access
- Remote database location
- Remove DS9 from reporter
- Service restart
- Setup new DS9
- Snmp data collection for flow device

Changes have been made to this configuration item

Setup new DS9

Base DS9 setup, configuration done on DS9 and dashboards and data sources created on reporter.

ds9IpAddress

Required - Ip address of DS9.

Add

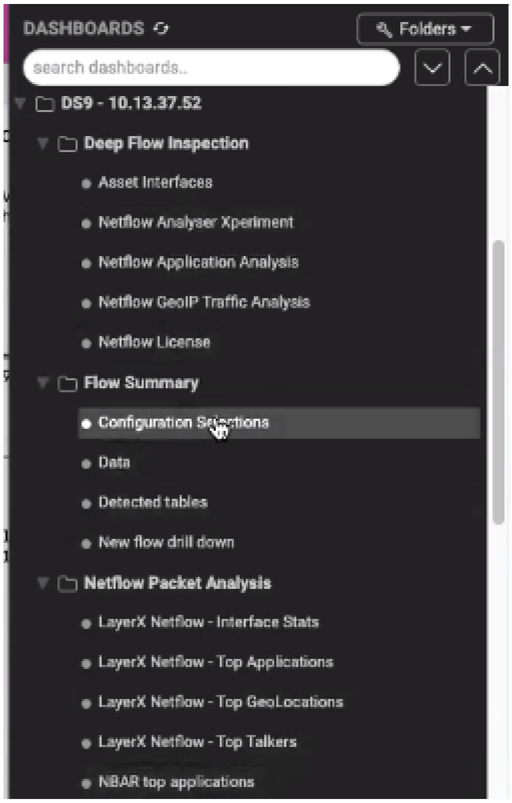
Add

To let the box know about the new datasources please refresh the browser. Use Display configuration option to confirm Remote database access to this reporter.

3. Refresh the Dashboard browser page and from the menu, select **Data Sources**.

   The new entries for the IP address are listed as `DS9 SNMP...`, `DS9 SUMMARY...` `DS9 TOPN...` entries.

4. Under the **DASHBOARDS** menu, the new **DS9 - <IP>** dashboard menu shows, for example:


DASHBOARDS

Folders

search dashboards..

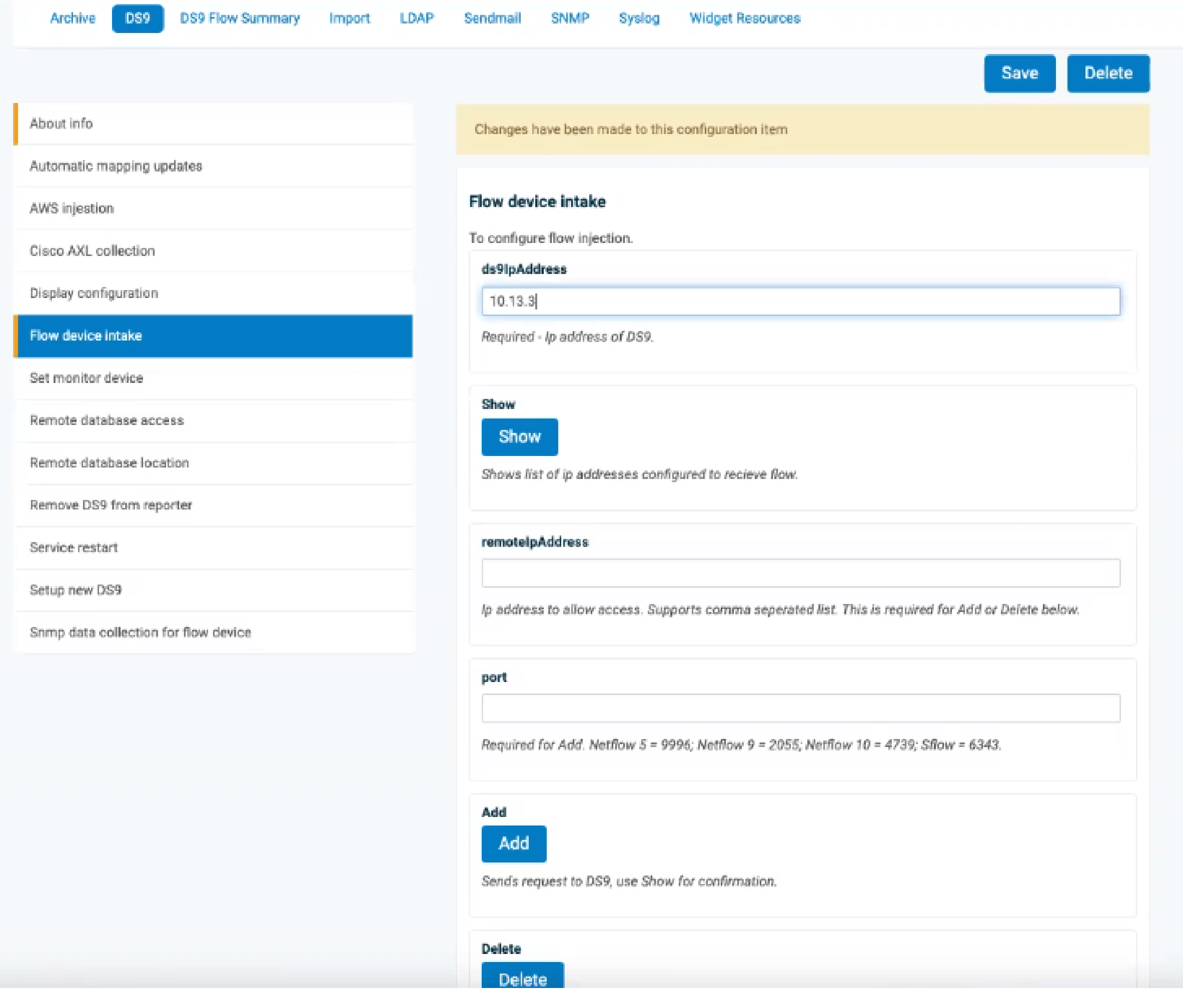
- DS9 - 10.13.37.52
  - Deep Flow Inspection
    - Asset Interfaces
    - Netflow Analyser Xperiment
    - Netflow Application Analysis
    - Netflow GeoIP Traffic Analysis
    - Netflow License
  - Flow Summary
    - Configuration Selections
    - Data
    - Detected tables
    - New flow drill down
  - Netflow Packet Analysis
    - LayerX Netflow - Interface Stats
    - LayerX Netflow - Top Applications
    - LayerX Netflow - Top GeoLocations
    - LayerX Netflow - Top Talkers
    - NBAR top applications

   Note at this stage the sub-menus are still empty.

5. Set up the Netflow devices for DS9. Go to **admin > Configuration** and on the **Configuration Settings**,

go to **DS9**.

6. Choose **Flow device intake** and for each remote netflow device that the DS9 server will receive flow data, set up **ds9IpAddress**, **remoteIpaddress** and **port** and click **Add**.



Changes have been made to this configuration item

Flow device intake

To configure flow injection.

ds9IpAddress: 10.13.3

Required - Ip address of DS9.

Show

Shows list of ip addresses configured to recieve flow.

remoteIpAddress

Ip address to allow access. Supports comma seperated list. This is required for Add or Delete below.

port

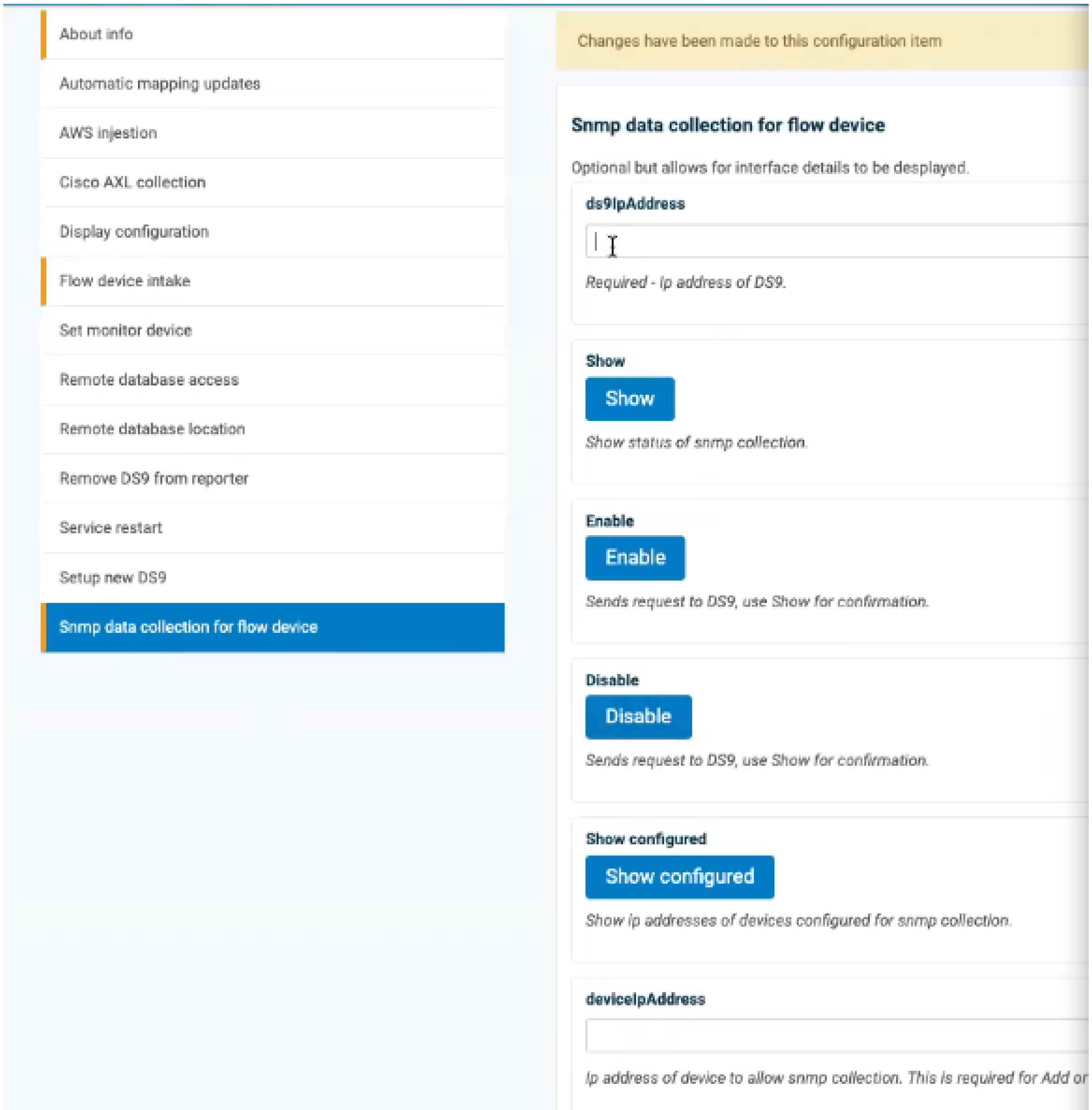
Required for Add. Netflow 5 = 9996; Netflow 9 = 2055; Netflow 10 = 4739; Sflow = 6343.

Add

Sends request to DS9, use Show for confirmation.

Delete

7. If SNMP data collection is also required, choose the **Snmp data collection for flow device** menu, enter data into the fields according to your configuration preferences and click **Add.** Repeat this step according to the number of flow devices set up.



Changes have been made to this configuration item

Snmp data collection for flow device

Optional but allows for interface details to be desplayed.

ds9IpAddress

Required - Ip address of DS9.

Show

Show status of snmp collection.

Enable

Sends request to DS9, use Show for confirmation.

Disable

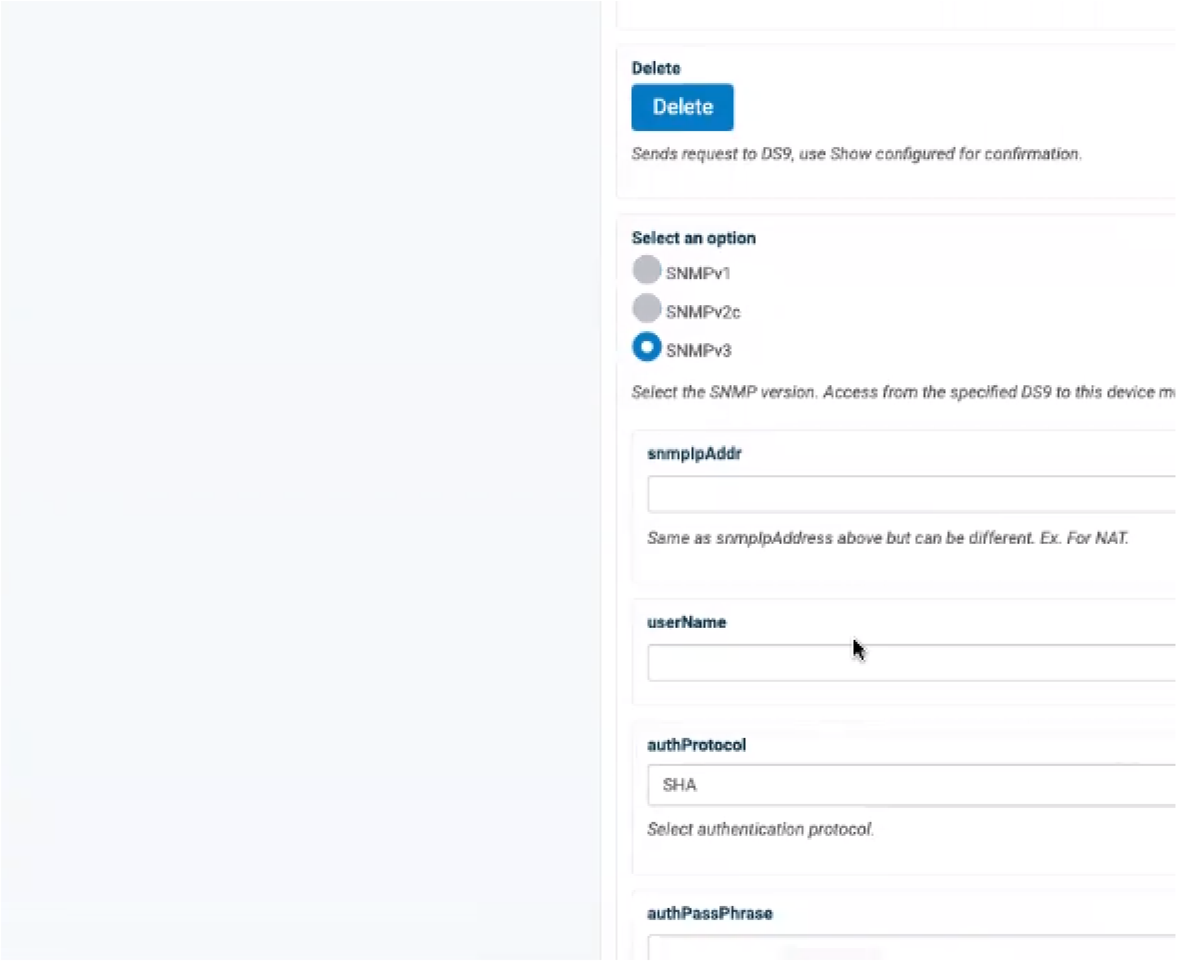
Sends request to DS9, use Show for confirmation.

Show configured

Show ip addresses of devices configured for snmp collection.

deviceIpAddress

Ip address of device to allow snmp collection. This is required for Add or



Delete

Sends request to DS9, use Show configured for confirmation.

Select an option

○ SNMPv1

○ SNMPv2c

● SNMPv3

Select the SNMP version. Access from the specified DS9 to this device m

snmpIpAddr

Same as snmpIpAddress above but can be different. Ex. For NAT.

userName

authProtocol

SHA

Select authentication protocol.

authPassPhrase