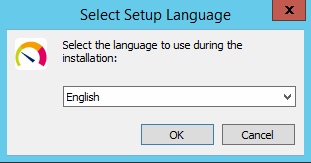


Please make sure the xx-monitor01 server has full internet access during this installation to ensure the License activation can be completed.

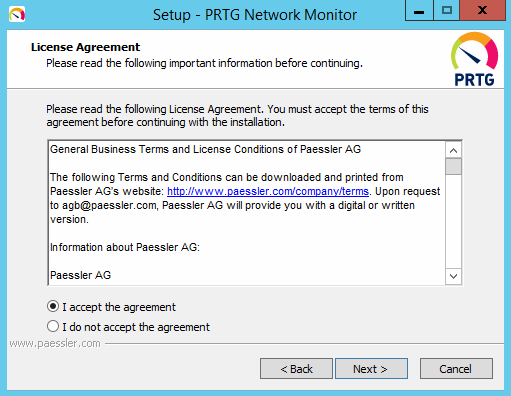
# PRTG software installation on server

PRTG Latest package can be found on: [\\jdn-file01\software$\Software - Windows Official\PRTG Network Monitor](file:///\\jdn-file01\software$\Software%20-%20Windows%20Official\PRTG%20Network%20Monitor\)

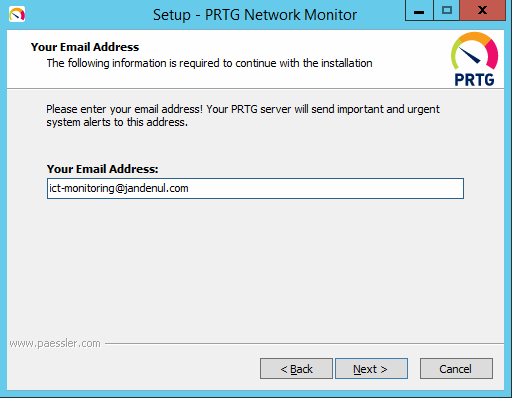
* Copy the following subdirectories to xx-monitor01:
  + PRTG - Configuration Files
  + PRTG - Office & small setup
  + PRTG - Software
* Run \PRTG - Software\PRTG Network Monitor 1X.X.X.XXX.exe



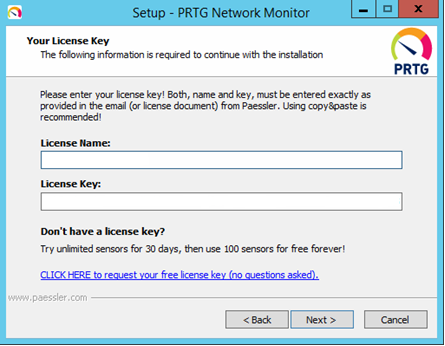
* Select ‘English’ and click ‘OK’

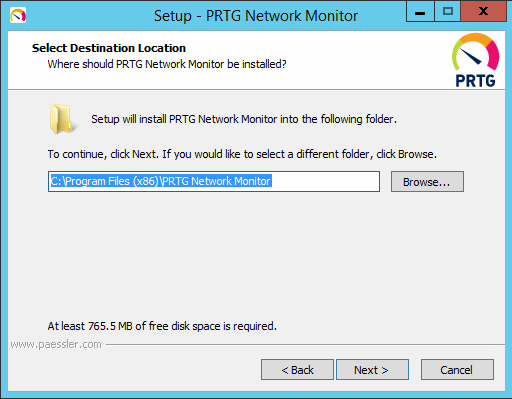


* Select ‘I Accept the agreement’ and click ‘Next’



* Fill in ‘ict-monitoring@jandenul.com’ and click ‘Next’

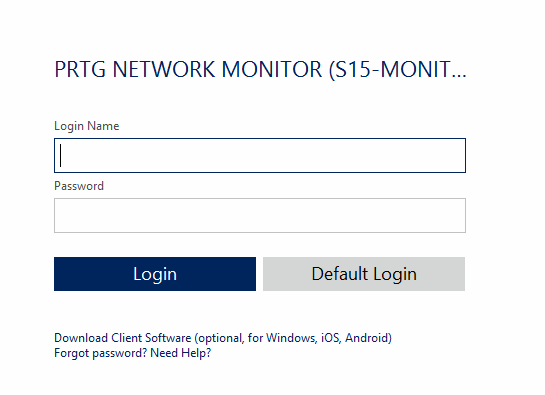


* Fill in the Name and License (check IT intranet vm-web02.jandenul.com)
* Click ‘Next’  
    
  
* Leave default installation Path and click ‘Next’

# PRTG Configuration

## Initial Configuration

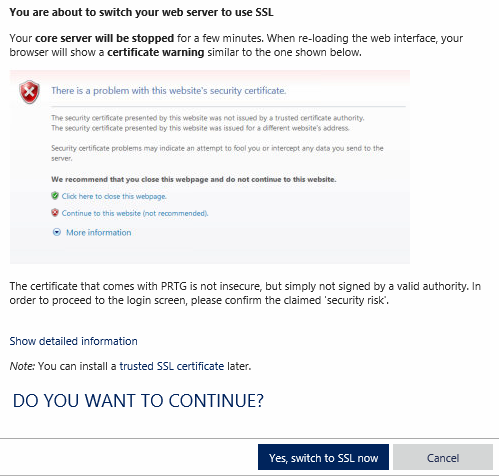
* After installation browse to <http://10.xxx.xxx.25> (use chrome or firefox on your management VM)
* Click Default Login



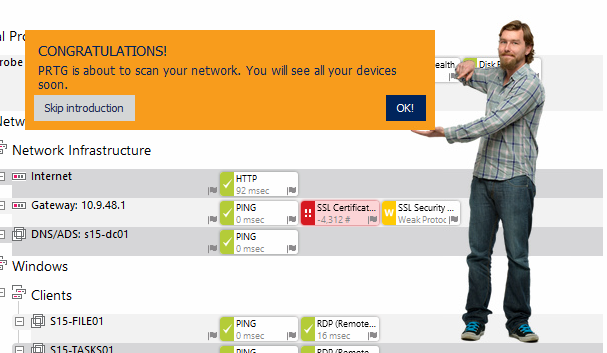
* Click Devices
* Click the ‘OK, switch now!’ button that the PRTG guy is holding.



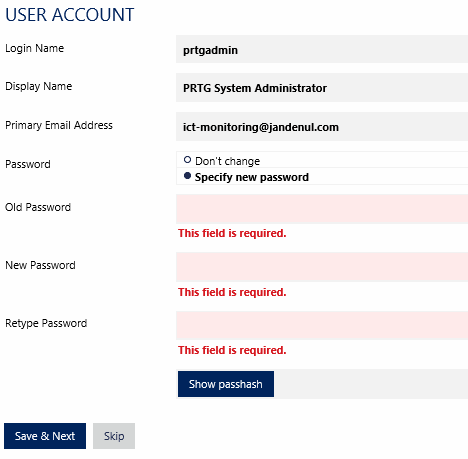
* You will receive the following pop up.



* Click ‘Yes, switch to SSL now’
* PRTG will now restart all the services, once restarted browse to <https://10.xxx.xxx.25>
* Click ‘Default Login’
* Click ‘Devices’
* Click ‘Skip introduction’

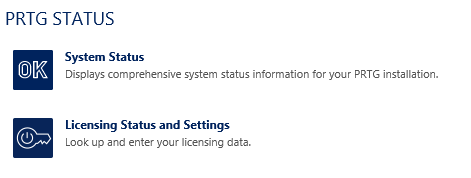


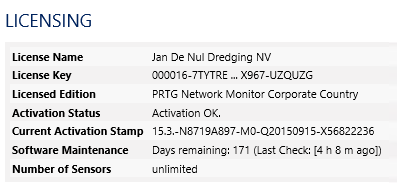
* Go to Setup
* Click My Account and check the radio button ‘Specify new password’



* Enter old password : prtgadmin  
  new password: SXXprtg”yearofinstallation” or “project code” (ex. VDprtg085)
* Click ‘Continue’
* Add the user and password to Remote desktop manager.

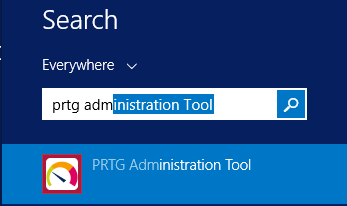
## Activation

* To check if activation is successful Go to Setup ==> Licensing Status and Settings  
  
* Check if Activation Status is Activation OK. (if not check internet connection and restart services)

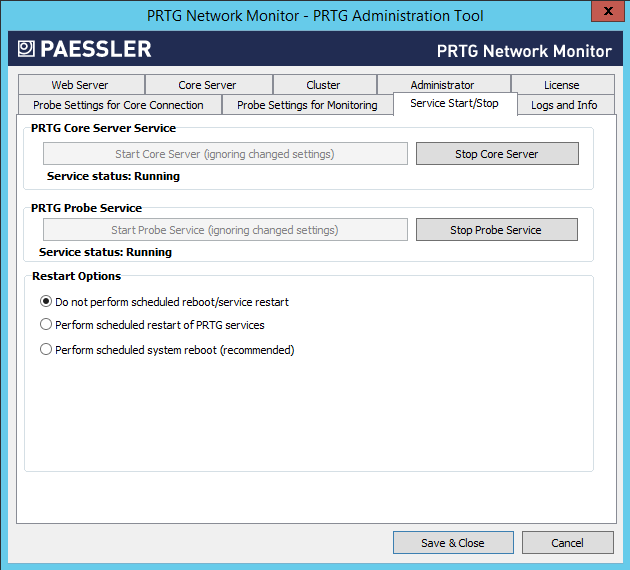


## Change Template Configuration file

* Open the PRTG - Configuration Files directory you copied in the first step of this manual
* Run the PowerShell script and follow the steps on the screen to generate a config file for your PRTG installation. Name the exported file 'PRTG Configuration.dat'
* Open PRTG Administation tool



* Go to tab Service Start / Stop

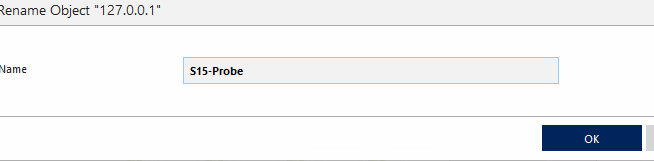


* Stop core server and probe service
* Copy newly created configuration file to C:\ProgramData\Paessler\PRTG Network Monitor
  + Copy and replace
* Start core server and probe service

## PRTG Settings

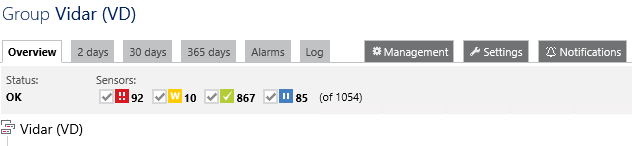
### Rename 127.0.0.1

* Right click on object 127.0.0.1 and rename to SXX-Probe



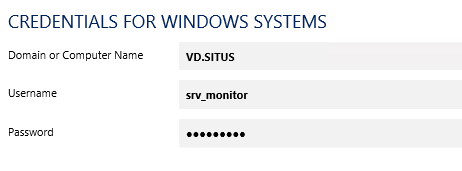
### General Settings

* Click on SXX (SXX)
* Go to ‘Settings’



#### Credentials for Windows Systems

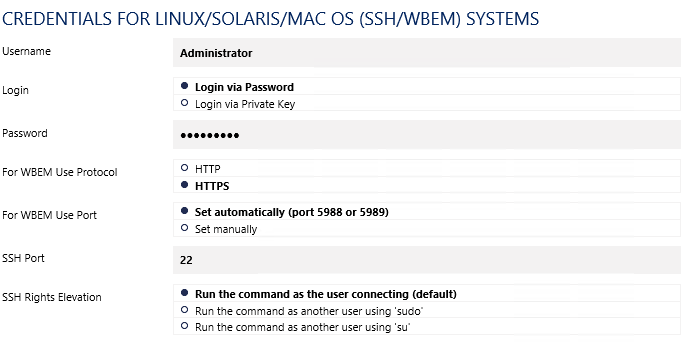
* Check/Change following settings



* NetBIOS Domain Name
* Username
* **Password**

#### Change Linux/Solaris/MAC OS (SSH/WBEM)

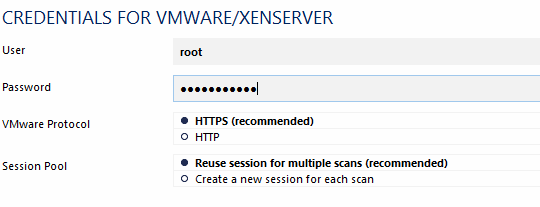
* Check / Change following settings



* + Username
  + **Password**

#### Change VMWare/Xenserver

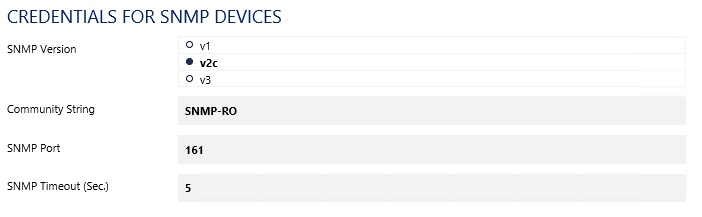
* Change following settings



* + User
  + **Password**

#### Credentials for SNMP devices

* This setting should be ok but check to make sure.



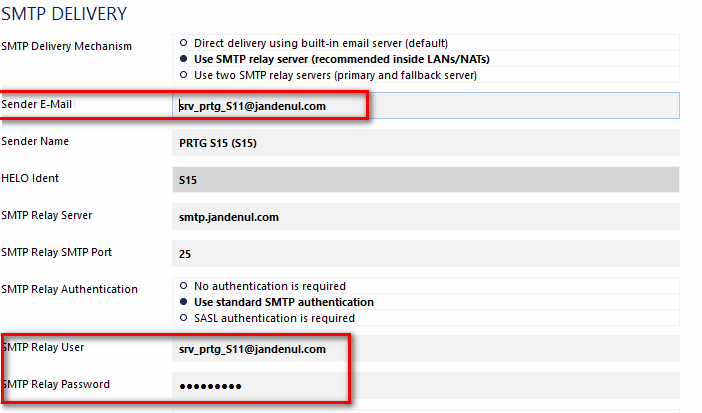
* SNMP-RO
  + Every device that is going to be monitored with PRTG through PRTG should get the appropriate SNMP string and version (if possible).

#### Virtual Servers Group

* For the group virtual servers the inheritance is broken because there is another username to authenticate in Vmware
  + Change the password to the correct one.
* Click the vcenter server device
  + Settings
  + Check the checkbox credentials for VMWare/Xenserver so it will inherit the correct credentials.

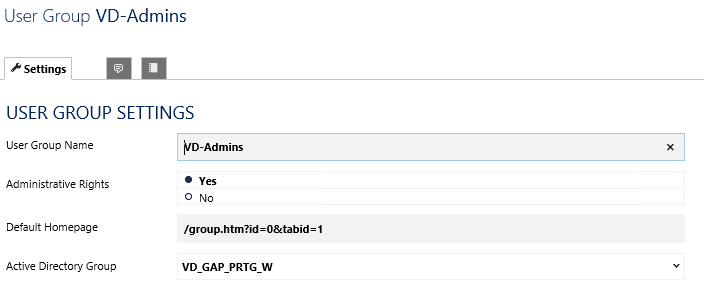
### Notification Delivery

* Go to Setup 🡺 Notification Delivery
* Please adjust the Sender E-mail and SMTP Relay user and password to the correct Small Case user.



### Users

* Go to Setup
* User groups
* Open XX-Admins and check that Active Directory Group is correct (XX\_GAP\_PRTG\_W) otherwise change this.



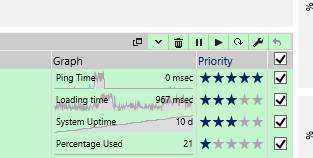
* Open XX-Users and check that Active Directory Group is correct (XX\_GAP\_PRTG\_R) otherwise change this.

# Setting up remaining Devices and sensors

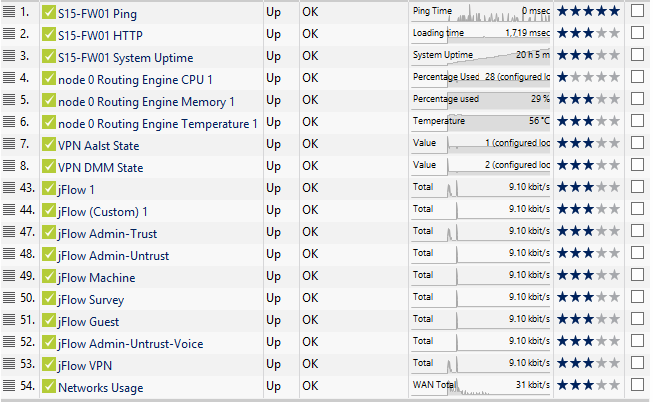
## Firewall (XX-FW01)

### Remove sensors and re-add them.

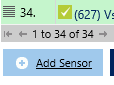
* + Select all Traffic sensors and click delete icon, confirm



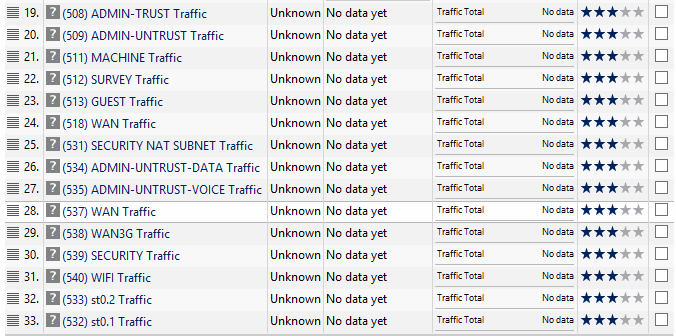
* + This is what you should have left



* + Click Add Sensor

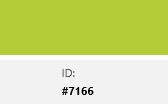


* + Add SNMP Traffic sensor, and select the sensors that you have a description plus st0.1 & st0.2.



### Networks Usage

* Click on each newly added WAN Traffic (bottom one) and write down the sensor ID you can find in the top right corner.



* Click on the Networks Usage sensor and then click Settings
  + Replace the channel ID with the one you just wrote down.

#100: WAN Total

Channel (9506, -1)

#107: VPN

Channel (9659, -1)

#101: Admin-Trust

Channel (9653, -1)

#105: Admin-Untrust-Data

Channel (9654, -1)

#106: Admin-Untrust-Voice

Channel (9658, -1)

#102: Survey

Channel (9656, -1)

#103: Machine

Channel (9655, -1)

#104: Guest

Channel (9658, -1)

### jFlow Sensors

Please ask SA/SE to reconfigure the Jflow on the SRX if all jFlow sensors have the same output.

Fill in the table below:

|  |  |  |
| --- | --- | --- |
| VVLAN | Range configured | Range needed |
| Admin-trust | 16 |  |
| Admin-untrust-data | 17 |  |
| Machine | 18 |  |
| Survey | 19 |  |
| Guest | 20 |  |
| Admin-untrust-voice | 21 |  |

* Select the first jFlow sensor Admin-trust
  + Click settings
  + Verify the ranges were configured correctly. If not, fix this.
  + In the exclude filter replace the numbers from ‘range configured’ column with the filled in by yourself column ‘range needed’.
  + Ex:   
    (DestinationIP[10.9.48-53.\*] AND SourceIP[10.9.48-53.\*]) OR

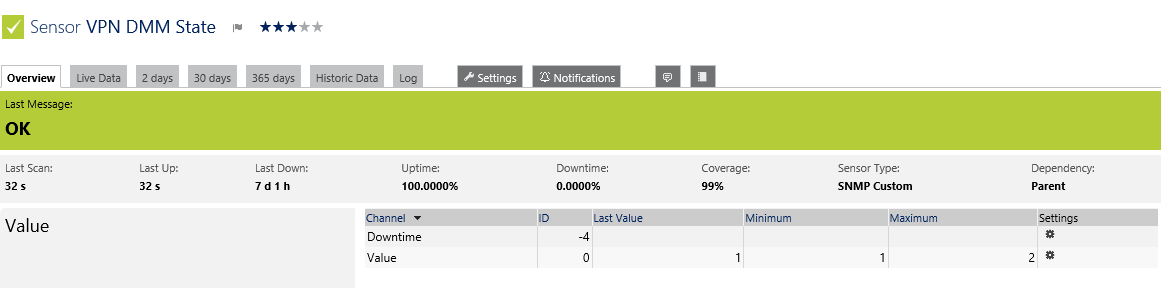
SourceIP[10.9.49-53.\*] OR

DestinationIP[10.9.49-53.\*]

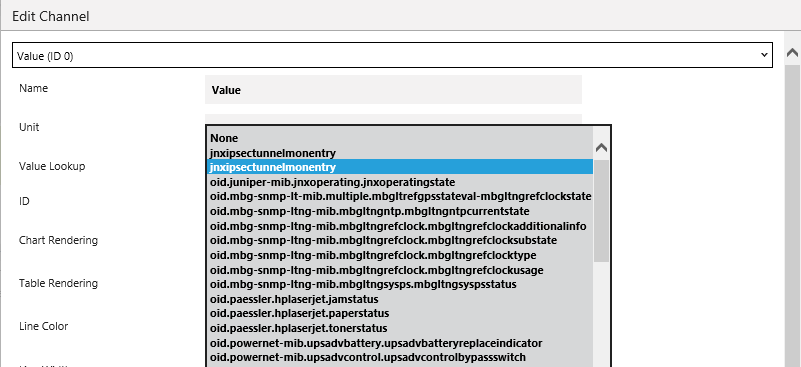
* Do this for every jFlow sensor (except jFlow and jFlow Custom)

### VPN Sensors

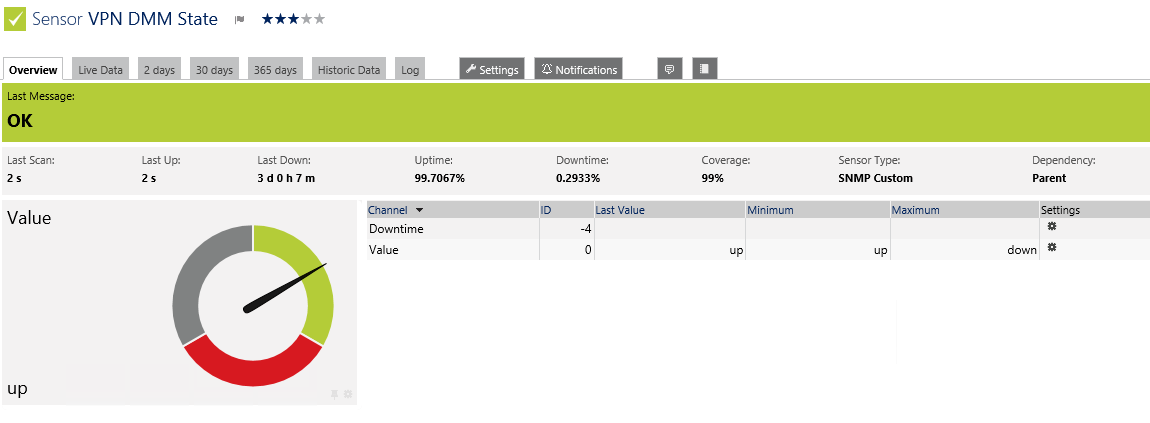
* For each VPN tunnel sensor (Aalst & DMM)
  + Select the VPN sensor



* + Click the Value channel edit symbol.
  + In Value lookup field select the first jnxipsectunnelmonentry from the dropdown list.

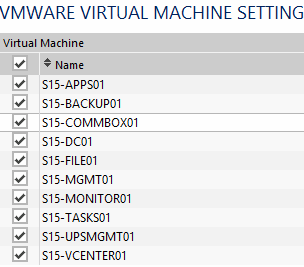


* + Click ‘Apply’
  + It should look like this.

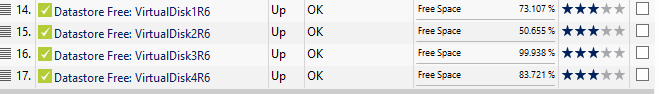


## Poweredge server (SXX-ESX01)

* Remove all VMware Virtual Machine SOAP sensors (for each VM on host)
* Re add Vmware Virtual Machine SOAP
  + Select all VM’s

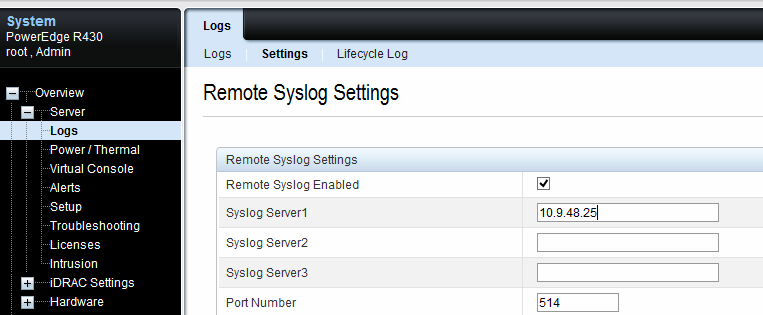


* Add Sensor 🡺 VMware Datastore SOAP

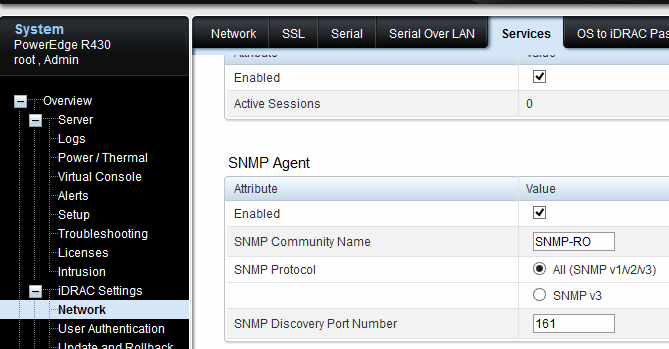


## IDRAC Sensor

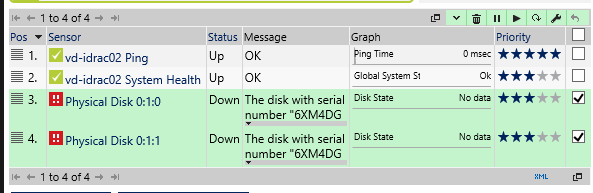
* Before you start please check the IDRAC settings that Syslog and SNMP is configured.
* Syslog
  + Logs 🡺 Remote Syslog Enabled check
  + Fill in Syslog Server 1: 10.XXX.XXX.25



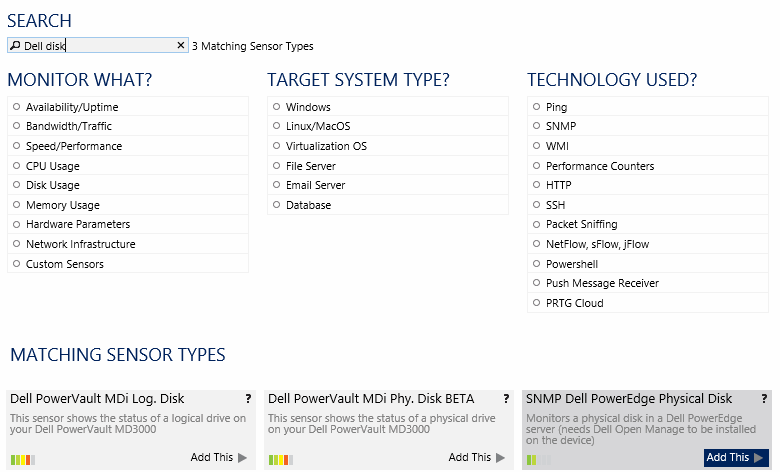
* SNMP
  + Community String: SNMP-RO



* Physical disk sensors will not work due to different serial numbers so they will have to be re-added.
* Select the IDRAC and select the physical disk sensors



* + Click the delete icon
* Click Add Sensor
  + search Dell disk



* + Add SNMP Dell Poweredge Physical Disk
  + Check all disks

If you receive an error, please restart your IDRAC

## vCenter

* Select the xx-vcenter01 device & go to settings.
* Remove the inheritance for “Credentials for VMware/XenServer” and add the administrator credentials.
* Remove all sensors except for Ping
* Add new sensor VMware host Performance (SOAP) (check option Virtualization OS)
  + Check esx host
* Add new sensor VMware host hardware Status (SOAP)
  + Check esx host
* Add new sensor VMware virtual machine (SOAP)
  + Check all virtual machines

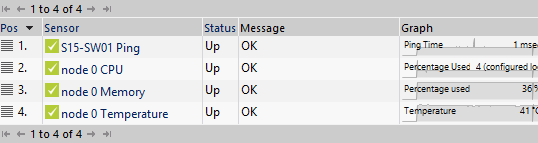
## APPS

If there is Amos is installed on the SC please resume the sensors of the apps server.

## Network

### SXX-SW01 node 0

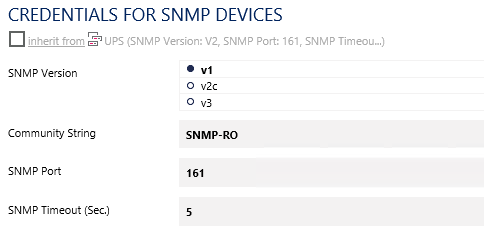
* Select all SNMP traffic sensors and delete them.
  + Remaining sensors



* Add SNMP Traffic sensors
  + Select all

## UPS (if present otherwise leave paused)

* Select the xx-ups01
* Click the settings tab
* Uncheck the ‘Credentials for SNMP Devices’ to disable the inheritence.
  + Switch SNMP version to v1

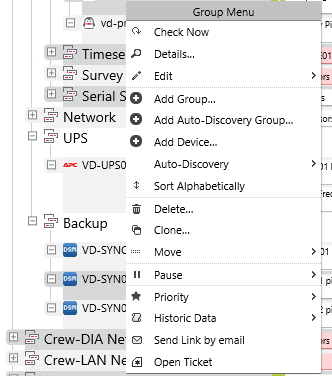


## Wifi AP

* Enable SNMP community string on the AP if not already done.

## Other groups (Crew-lan & DIA, Machine, Survey)

* Remove all devices
* Run auto discovery
  + Rightclick on group ==> Auto-Discovery ==> run auto-discovery

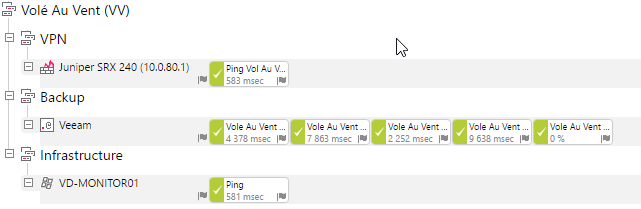


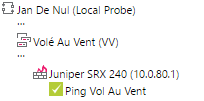
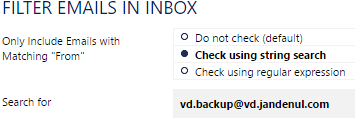
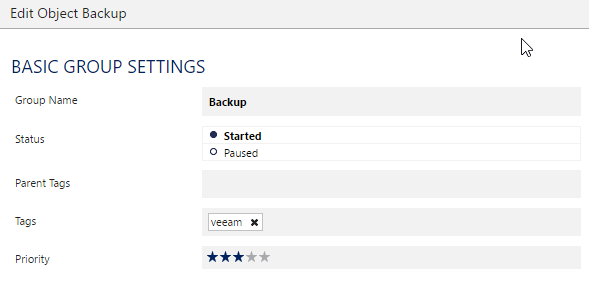
# Change JDN PRTG

## JDN-PRTG02

Login to <https://jdn-prtg02.jandenul.com>

Clone the following devices from **Volé Au Vent (VV)** to your Vessel/Office device.



* Juniper SRX 240 (10.0.80.1)
  + Change the juniper model if needed.
  + Change the ip-address to you firewall ip-address
  + Change the name of the ping sensor to “Ping <vessel/office name>
* VD-MONITOR01
  + Change the device name to your vessel/office abbreviation XX-MONITOR01
  + Change the IPv4 address
  + Change the Dependency to the ping sensor of the Juniper SRX 
* Backup
  + Change the imapsensor name with the vessel/office name
  + Change the “Filter emails in inbox > search for” to your vessel/office abbreviation 
  + Add the “veeam” tag to the Backup group

If the new setup is already in production. Cleanup all the old sensors. If the old setup is still in production, remove them after the swap.

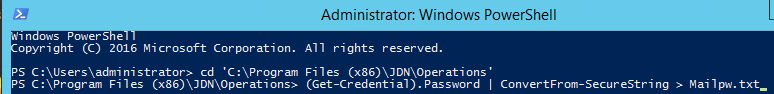
# Snapshot Search Script

Copy the latest versisio of the script from: **\\Jdn-file01\ict\_new\_standard\_sites\_vessels\Other\Check for snapshots** to XX-MONITOR01 **C:\Program Files (x86)\JDN\Operations**

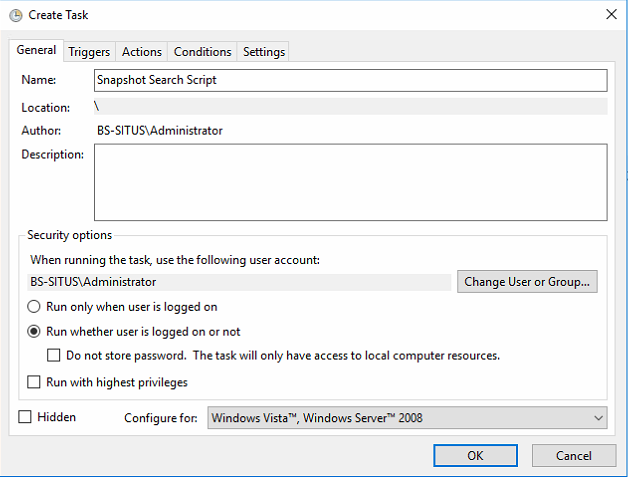
Edit the script variables with the parameters of the vessel



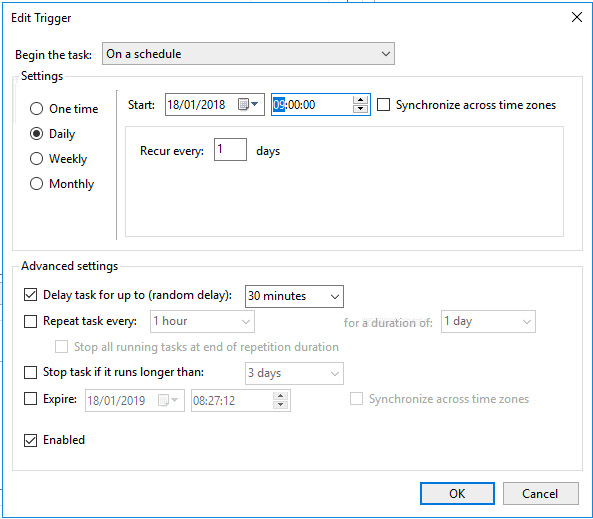
Add the vcenter credentials with Powershell  
**New-VICredentialStoreItem -Host 10.X.X.10 -User 'administrator@vsphere.local' -Password 'password'**

Add the srv\_backup\_XX password to encrypted file  
**(Get-Credential).Password | ConvertFrom-SecureString > Mailpw.txt**

Create a new Scheduled task.



Create a new Trigger



Create a new Action

Arguments:   
**-ExecutionPolicy Bypass -File "C:\Program Files (x86)\JDN\Operations\SnapshotSearchReport.ps1"**

