User Guide

RS9 Management Access

- RAID Controller
- Server

Published June 2021

Fibrenetix believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Fibrenetix disclaims all warranties, express or implied, including, without limitation, those of merchantability, fitness for a particular purpose with respect to contents of this User's Manual. Users must take full responsibility for the application of the product.

Fibrenetix, and other trademarks are trademarks of Fibrenetix or its subsidiaries. Other trademarks may be the property of their respective owners.

Fibrenetix
Langebjerg 23B
4000 Roskilde
DENMARK

http://www.fibrenetix.com

Do not dispose this electronic device into the trash while discarding. Please recycle to minimize pollution and ensure environment protection.

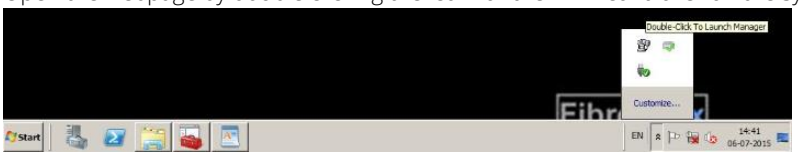
Table of Contents

Fibrenetix RS9 Server RAID Controller Storage Management

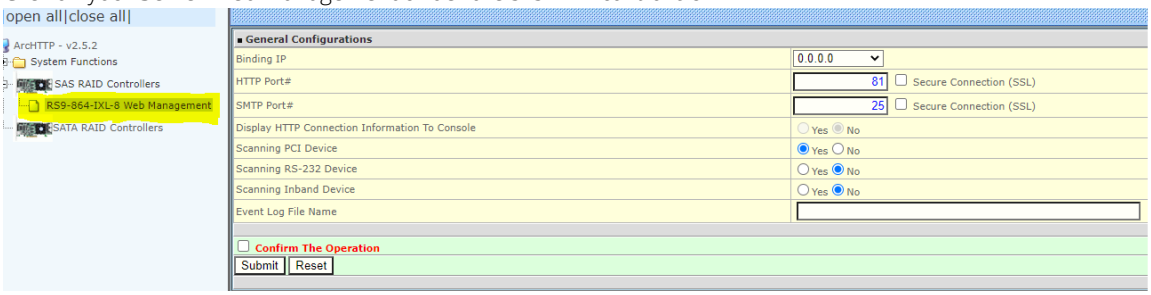
The Fibrenetix RS9 Web Based RAID Management allows a system administrator to Configure as well as monitor system health and manage computer events remotely. User can manage the RAID subsystem via standard web browsers connected to the RJ45 LAN Port.

Two Methods to Access the Web Based GUI on the Server.

- Open the webpage by double clicking the icon for the RAID controller on the system tray



- Click on your Server Web management under the *SAS RAID controllers*

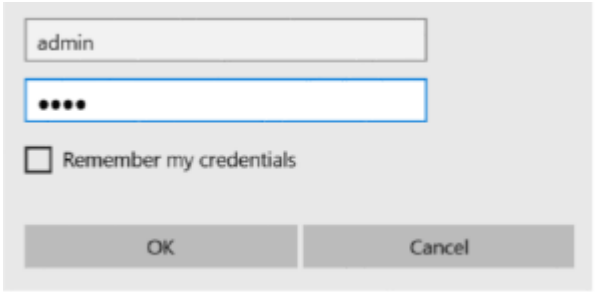


or

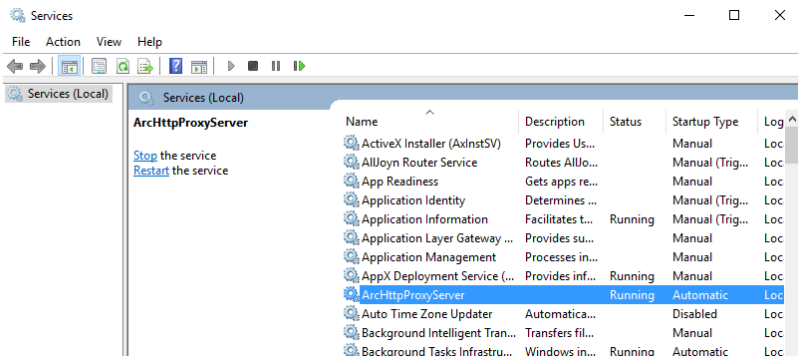
- Enter the IP address in the web browser with the local host as IP address `127.0.0.1:82` or enter `http://[MACHINE_IP_ADDRESS]:82`

Default Credentials

- Username: "admin"
- Password: "0000

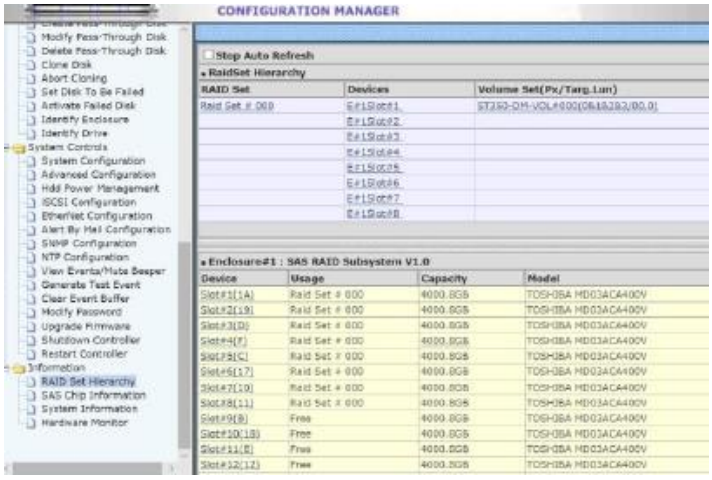


Note: Make sure that the *ArcHttproxyServer* Service is running in Services



Web Browser Management

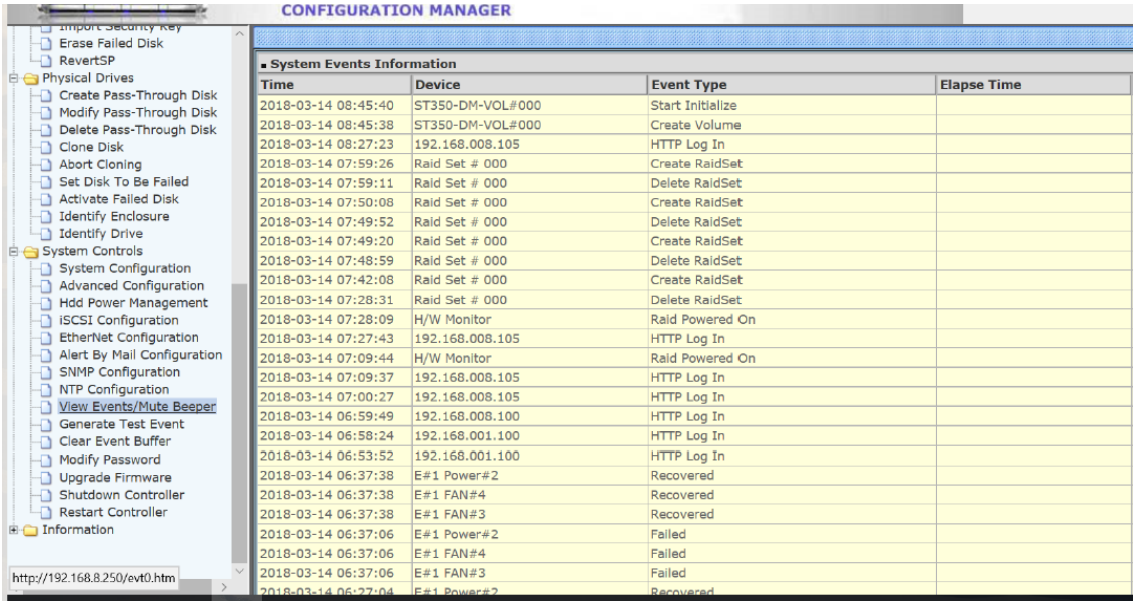
The startup screen displays the current configuration of the RAID subsystem. It Displays the RAID set list, volume set list and Physical Disk list.



Event Log

To view the RAID subsytem's event information go to *system Controls->view Events/ mute Beeper*

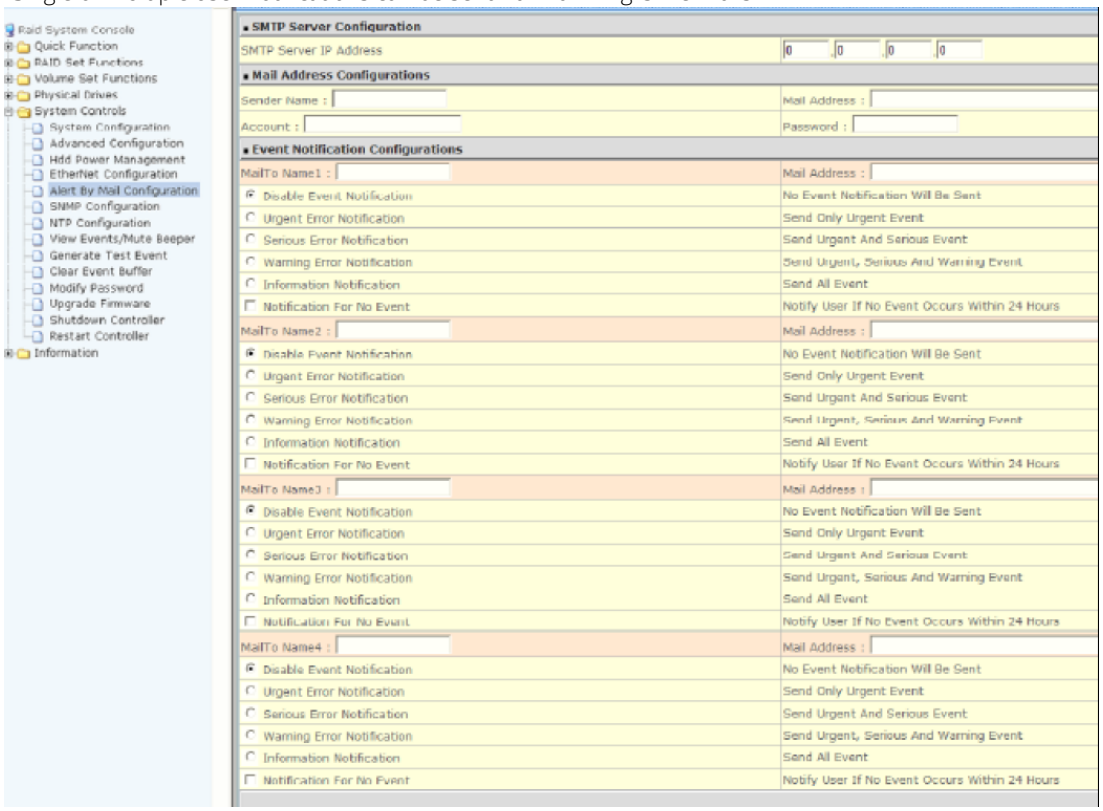
- This function automatically enable by clicking on the "*view Events / Mute Beeper*"



E-mail Alert

User can send alert via email by configuring the SMTP

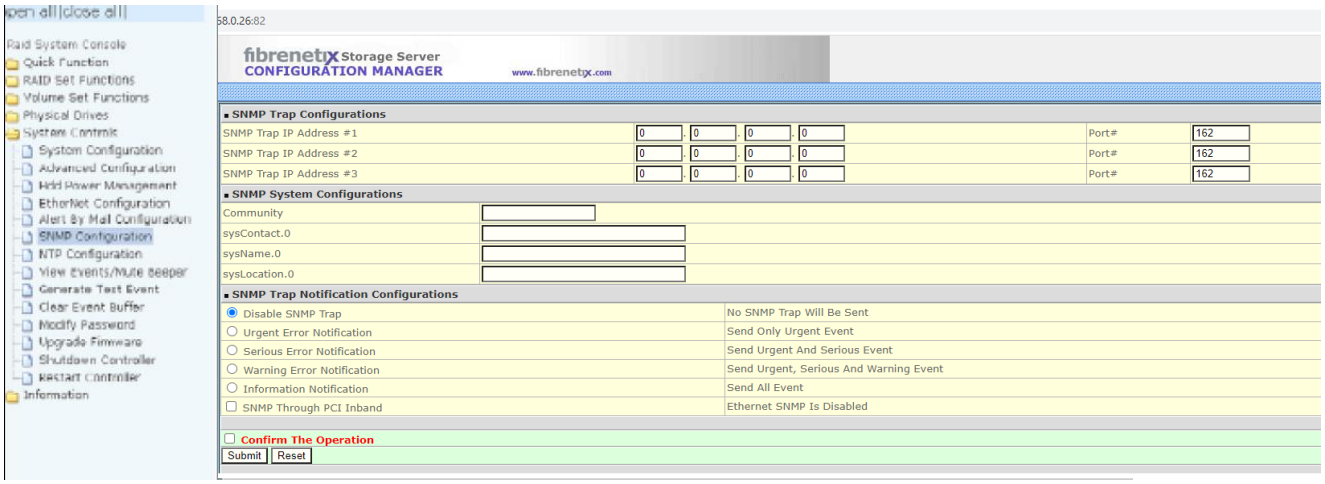
•click on the "System Controls" link
•Move the cursor bar to the "Alert By Mail Configuration" item
•then select the desired function
•The firmware contains a SMTP manager monitoring all system events
•Single or multiple user notifications can be sent via "Plain English" e-mails



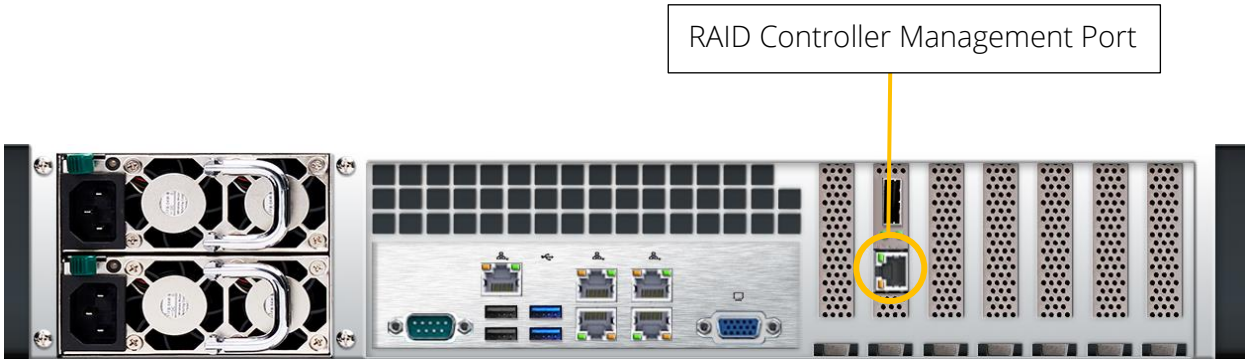
SNMP Configuration

To configure the RAID subsystem's SNMP function, select System Controls > SNMP configuration.
The firmware contains SNMP agent manager monitors all system events and user can use the SNMP function from the web settings.
This function can only set by the web-based configuration

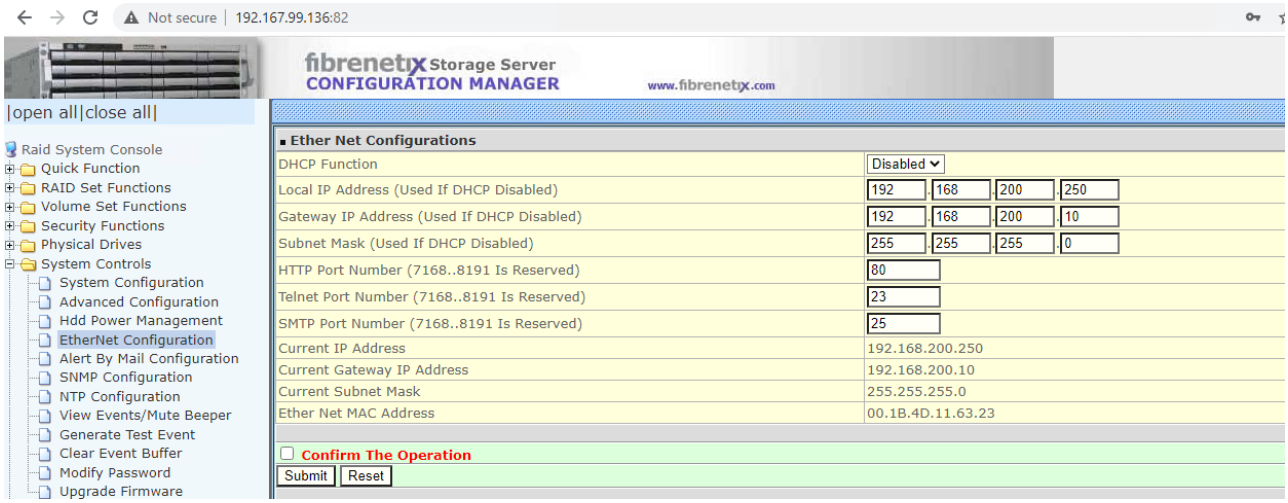
- Enter the SNMP Trap Address
- Community name acts as a password to screen accesses to the SNMP agent. Enter community names of the SNMP agent. Before access is granted, this station must incorporate a valid community name into its request; otherwise, the SNMP agent will deny access to the system. Most network use "public" as default community names.



Raid Controller management Access via LAN



To remotely access the raid control management via LAN network, we need to setup the Ethernet configuration IP addresses. This webpage will be accessible on the remote servers on the LAN within the same IP subnet.



Fibrenetix RS9 Server Administration

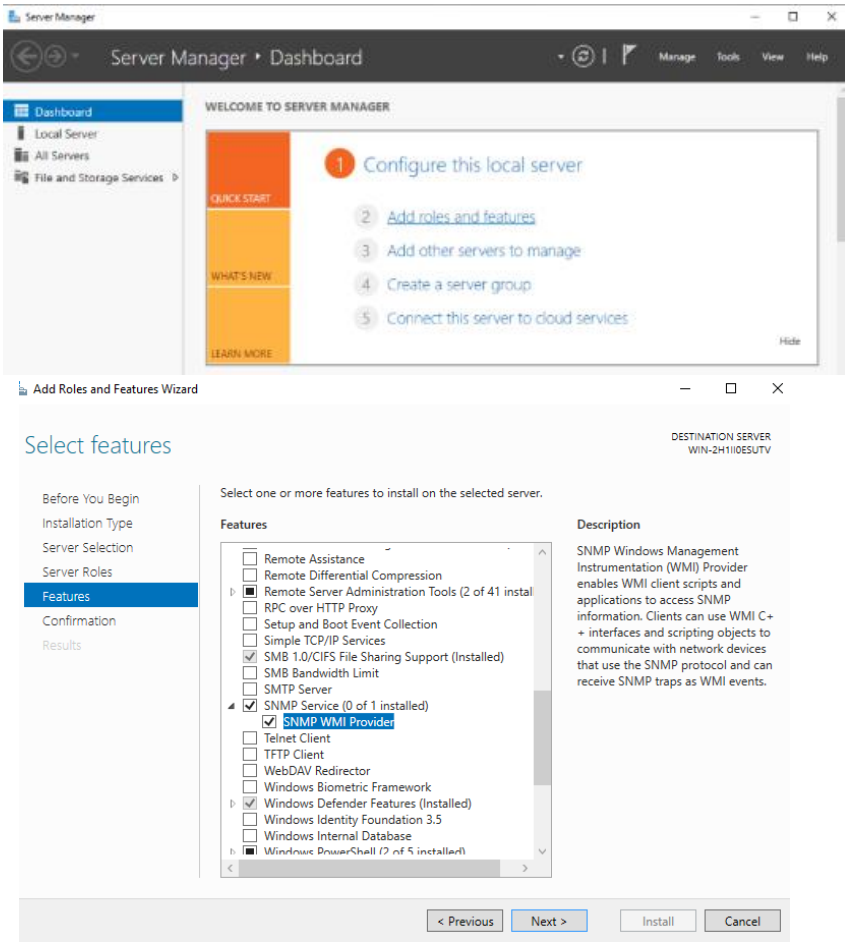
The Fibrenetix RS9 Server management administration using Super Doctor (SD5) helps the user the monitoring, control, and management functions. It helps the Hardware Monitoring: fan speed, temperature, voltage, chassis intrusion, redundant power failure, power consumption, disk health, raid health, and memory health also Provides SNMP extensions for network management system.

SD5 contains an SNMP extension module that should be plugged in into the Microsoft Windows SNMP service. Users can therefore query the readings of monitored items via SNMP.

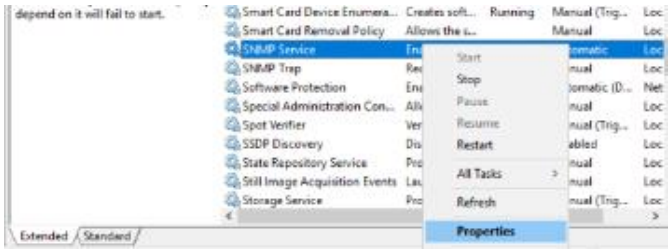
Note: To install the SNMP extension, the Microsoft Windows SNMP service must be installed first.

Configuring SNMP Services on Windows Server

1. Open Server Manager, ***Add roles and features*** and proceed installation until you reach the Features page. Check the **SNMP Service** in the list of features.



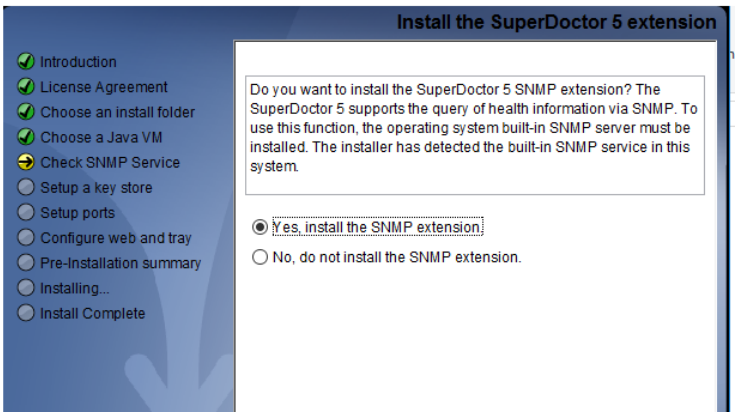
2. Select the SNMP Service then Install the installation process will start.
3. Open the Services window, find the SNMP Service, and open Properties. On the General tab, be sure to select Automatic in the Startup Type section so that it is always available even after a restart of the Server



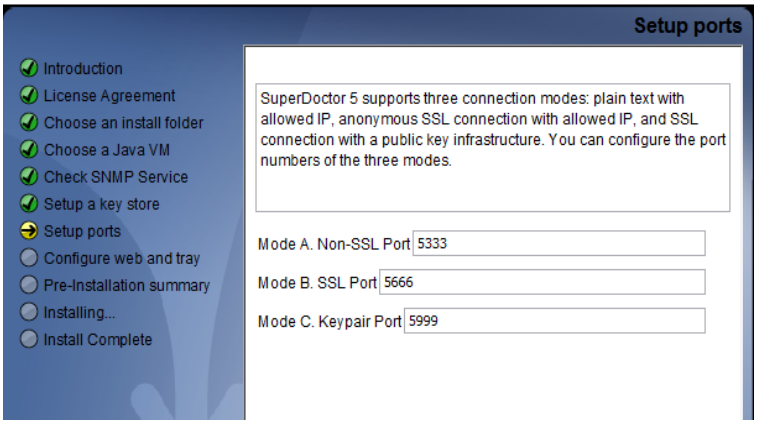
Installing and Configuring SuperDoctor5

By Default RS9 Servers are installed with superDoctor5 software, with SD5 shortcut on the desktop.
If required to Install contact Fibrenetix for the download link. Below are the installation steps.

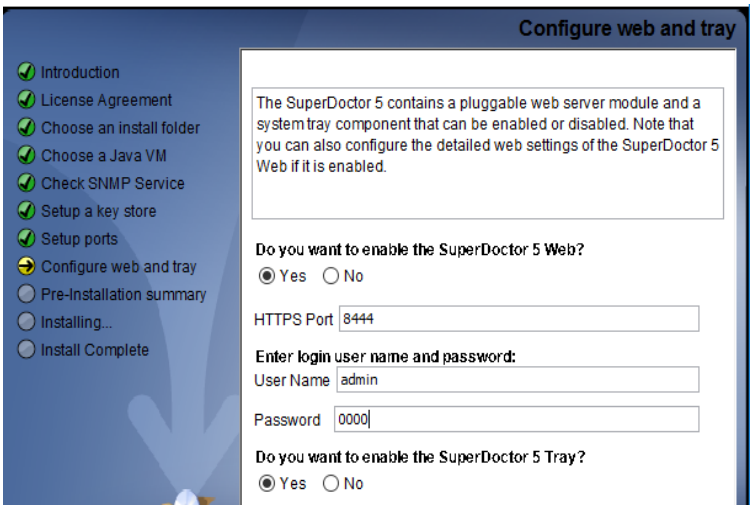
1. Execute the SD5 installer. Note that you must have Administrator privileges to install and run SD5.
2. During Installation, If the Microsoft Windows SNMP service is installed, you can either:
    - install the SD5 and the SNMP extension,



3. Select Yes to use the default key stores and click the Next button to continue
4. Three communication modes are supported in and by default, Mode B (SSL) and Mode C (Keypair) are enabled when SD5 is installed. You can configure the port numbers. Click next to continue.



5. SD5 provides the Web console "SD5 Web", Select Yes to enable the SD5 Web. You can also configure the default HTTP port number and the default HTTPS port number to access the SD5 Web. When completed, click the Next button to continue.

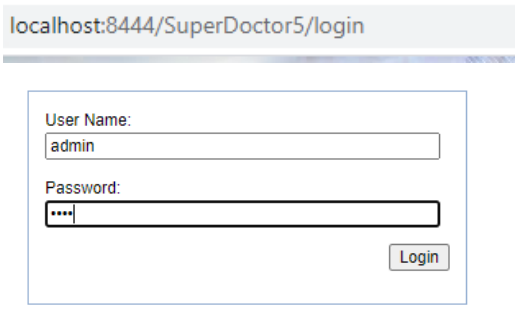


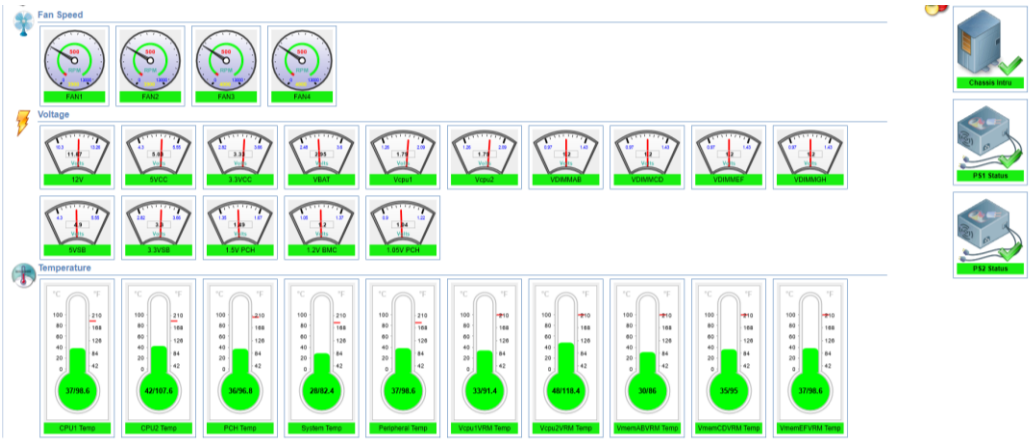
6. Once Installation complete, Click the Done button to exit.

Web Based Server Monitoring

SD5 Web graphically displays the status of the monitored devices, including fan speed, voltage, temperature, chassis intrusion, power failure, hard disk drives, and memory. An item in green color indicates a healthy state while a red one denotes a critical state. Notifications can be sent when a monitored item reaches critical status

1. Login to the local web browser as shown below and enter the login Username and Password





The health information page also shows power supply information if supported power supplies are connected to the motherboard via I2C. Depending on their design, power supplies might have Field Replaceable Unit (FRU) Data and/or PMBus functions.

Different colors are used to indicate the battery state. Green color means the battery is healthy, and red color means the battery is dead. If the current reading of the battery is negative, the color turns yellow to warn that the battery is discharged. In addition, the energy reading tells the percentage of the charge status of the battery.

The health of a RAID controller is a combined status that depends on the states of its components such as battery backup unit (BBU), virtual drives, and hard disks. If all components belonging to the adapter are OK, the status of the adapter shows OK. Otherwise, it could be Warning or Critical depending on the states of the components.

Alert Configuration

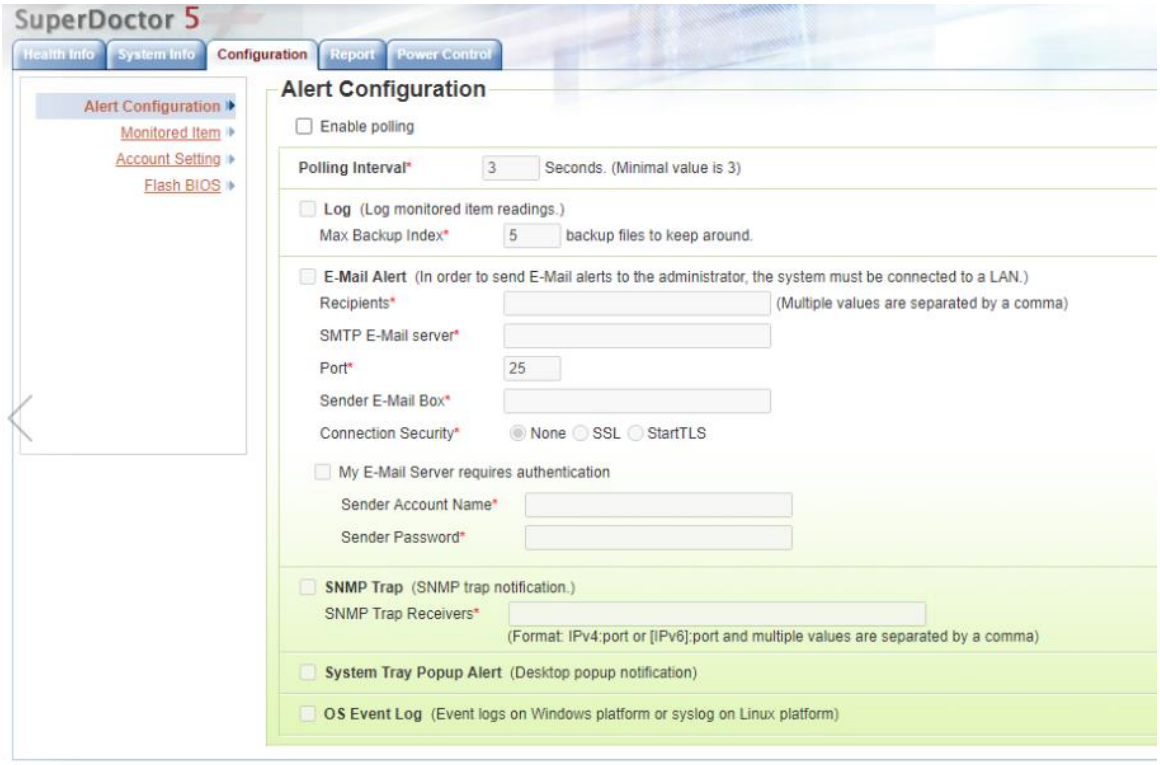
Note: A problem alert will be sent while the status of the monitored item is non-OK (i.e., WARNING, UNKNOWN or CRITICAL) from the initial or is from an OK state to a non- OK state or is from a non-OK state to another non-OK state. A recovery alert will be sent while the status of the monitored item is from a non-OK state to an OK state

Four methods are supported: Log, Email, SNMP Trap and System Tray

Note: Enabled Pooling: periodically checks the health status of monitored items if pooling is enabled. No alert is sent if pooling is disabled.

- Polling Interval: Determines how frequently in seconds the SD5 Web should check the health status of monitored items. The minimum value is 3 seconds.
- Log: Keeps alerts in a log file named "log.txt[yyyy-mm-dd-sequence]" located in the [install folder] folder. The file is split into two files once its size becomes greater than 10 MB. The total number of log files to be kept can be configured by setting the "backup files to keep around" argument.
- E-mail Alert: Sends alerts via e-mail. To use this function, you need to set recipients, an e-mail server address and a port number as well as a sender's e-mail address. Check SSL or TLS if the e-mail server uses secure connections. If the e-mail server requires authentication, you will need to set up an account and password to log in to the e-mail server. Multiple recipients must be separated by a comma.
- SNMP Trap: Sends alerts with SNMP traps. Multiple recipients are separated by a comma.

- System Tray Popup Alert: Sends alerts to local desktop. Note that the function is only available on Windows platform.



The E-mail message Configuration

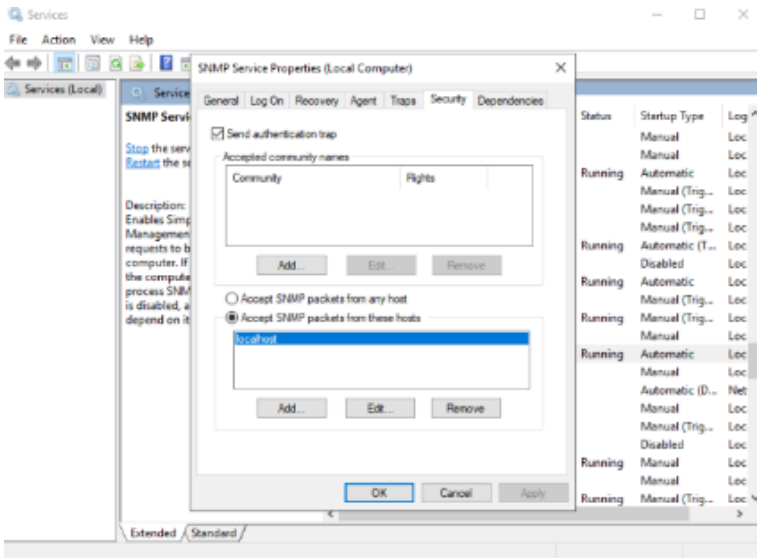
The E-mail message format is defined by the following attributes:
Mail title:
Item 1: the type of an alert ("Problem ", "Recovery ")
Item 2: the name of the monitored item
Item 3: the status of the monitored item ("OK", "Warning", “Critical”, or "Unknown")
Item 4: the time of an alert in date time format
Item 5: the host name and host address which sent out an alert
Mail body:
Item 6: the output message about the status of the monitored item

The SNMP Trap description

The SNMP Trap description if defined by the following attributes:
Item 1: the type of an alert ("Problem", "Recovery")
Item 2: the name of the monitored item
Item 3: the status of the monitored item ("OK", "Warning", “Critical”, or "Unknown")
Item 4: the time of an alert in date time format
Item 5: the output message about the status of the monitored item

Configuring the SNMP Service

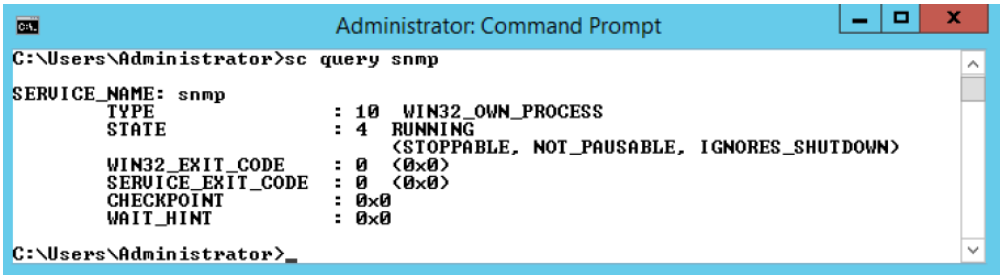
- Open the Control Panel. Click Administrative Tools. Click Services. Select the SNMP Service.
- Double-click the SNMP Service, and the SNMP Service Properties dialog box appears.
- Click the Security tab. In the Accepted community names setting, click the Add... button to add a public community with READ ONLY rights. Select Accept SNMP packets from any host.
- Click the OK button to complete the settings.



- Just click OK and then restart SNMP Service.

Verifying the SNMP Service

- You can use sc query snmp to check the SNMP service in console mode.



Report

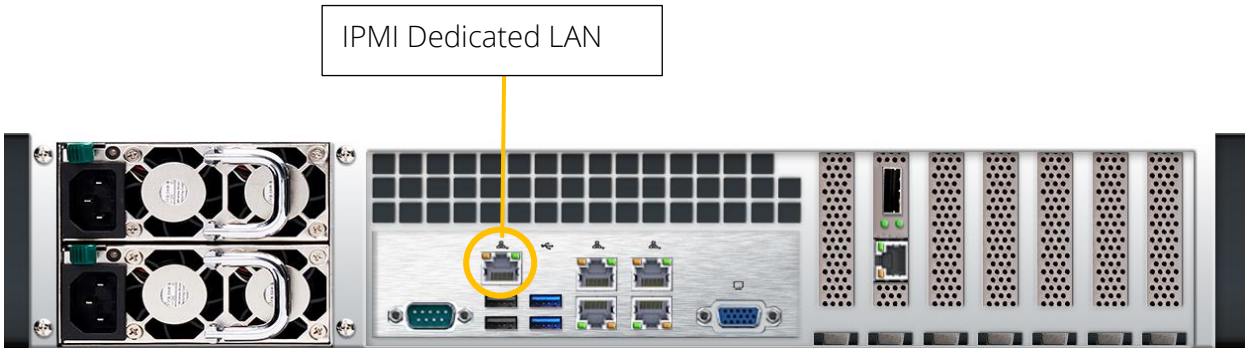
It Provides three CSV (Comma Separated Values) format reports. These reports can be downloaded and viewed with CSV supported tools like Microsoft Excel.

- System Information Report: This report contains information shown in the System Info function.
- Health Information Log Report: This report includes the historical data of monitored item readings. Readings of selected (i.e. enabled) monitored items will be written to a file only if the Polling Interval value is set and the Log option is enabled in the Alert Configuration function.
- Event Log Report: This report contains events that represent problems and recoveries with monitored items. When the status of a monitored item is changed, an event log is written to the Event Log Report. Note that to write events to the log file, the Polling Interval on the Configuration page must be set.

IPMI LAN Management

A Dedicated IPMI LAN Port is located on the back panel of the RS9 Server, that accepts RJ45 Cable.

It allows a system administrator to monitor system health and manage computer events remotely.



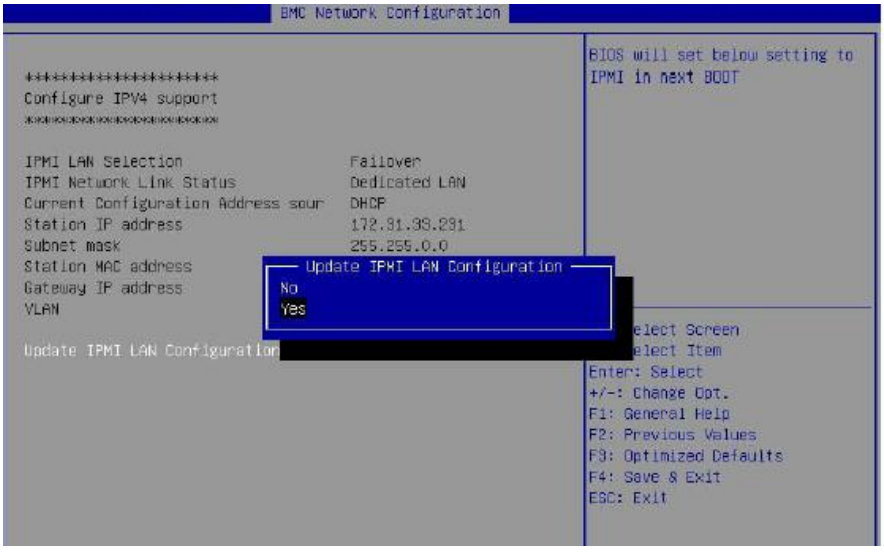
Configuring BIOS

For the IPMI to work properly, please enable all onboard USB ports and the COM port designated for SOL (IPMI) on the motherboard. All USB ports and the COM port for IPMI (marked with "*") are **enabled** in the system UEFI BIOS by default. It is usually listed as COM2 or COM3 in the UEFI BIOS.

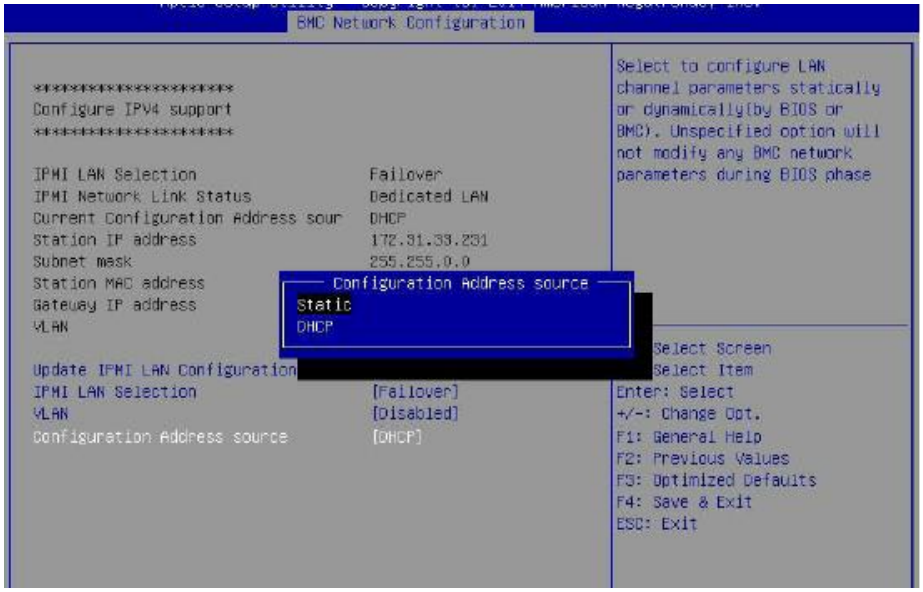
The default network setting is "**Failover**", which will allow the IPMI to connect to the network through a shared LAN port (onboard LAN Port 1 or 0) or through the IPMI Dedicated LAN Port. If the IPMI must be connected through a specific port, please change the LAN configuration setting under the Network Settings.

To verify and Configure follow the below steps

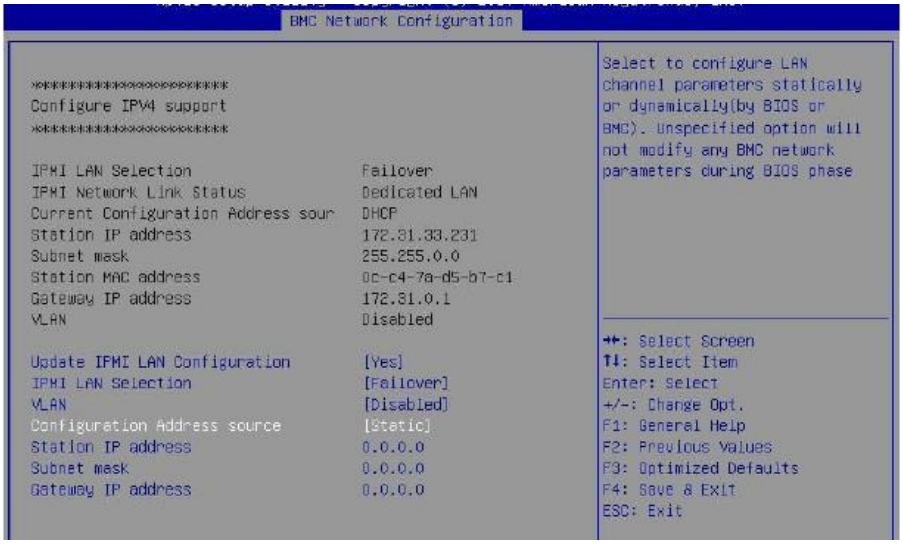
1. During the system bootup, press the <Del> Key to Enter the UEFI BIOS
2. During the system bootup, press the <Del> key to enter the UEFI BIOS.
3. Select the *IPMI* tab.
4. Select *BMC Network Configuration and* press <Enter>.
5. Highlight *Update IPMI LAN Configuration,* press *<Enter>* and select [Yes].

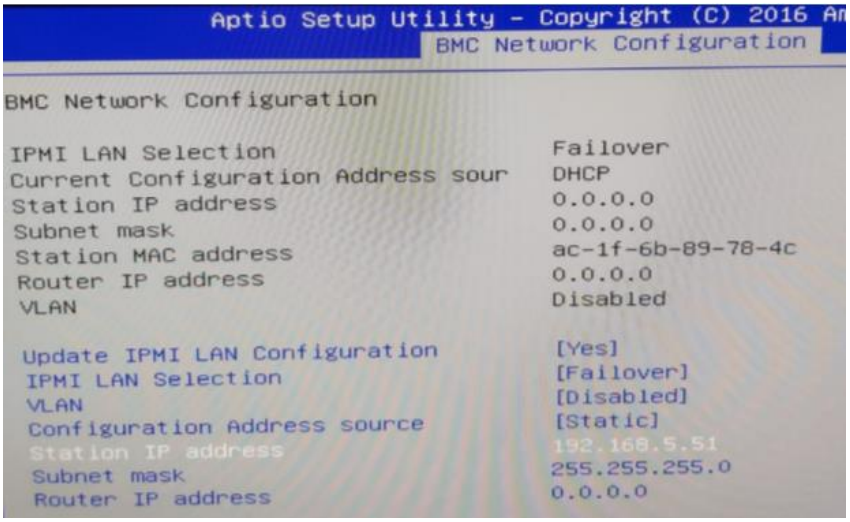


6. Highlight *Configuration Address Source* and select [Static].



7. Once the *Configuration Address Source* is set to [Static], the *Station IP Address, Subnet Mask* and *Gateway IP Address* fields will display *0.0.0.0,* which indicates that these fields are ready for you to change to new values. Select each of the three items and enter the values. Press <Enter> when finished.



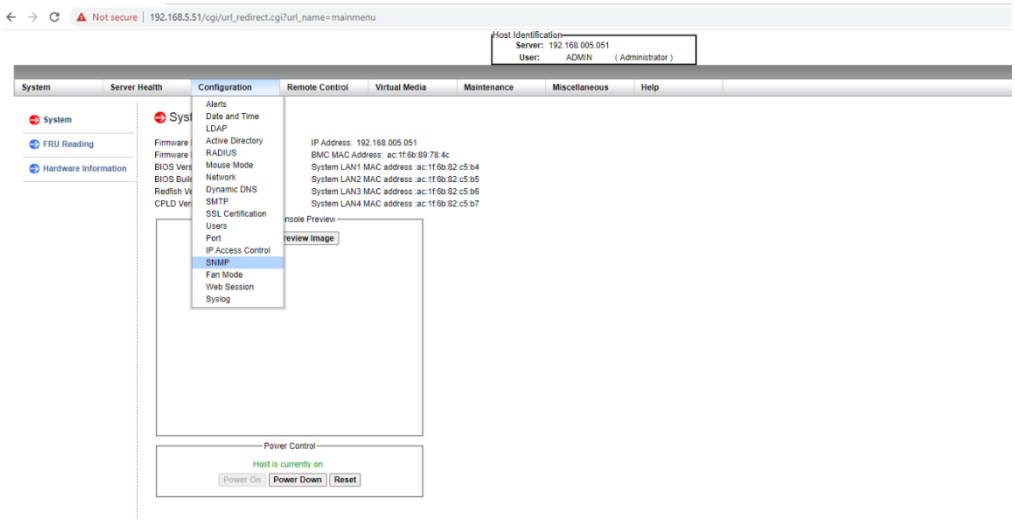


Accessing the Server Using the Browser

1. open a web browser. Enter the IP in URL bar and you will see a login screen.

Enter the username, **ADMIN**, and the password, **ADMIN**.

- Main screen displays The Menu bar: The menu bar on the top displays the System Information, Server Health Configuration, Hardware Information, Remote Control, Virtual Media, Maintenance, Miscellaneous, Help.

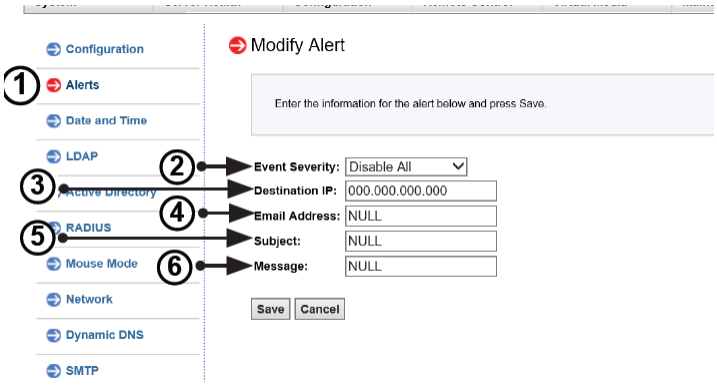


Alert Configuration

This feature allows the user to configure *Alert* settings. When you click on *Alerts* in the menu bar.

To setup an alert or to modify an alert setting, do the following.

1. Click on <Alerts> to activate the alert submenu.
2. Click on <Modify> to configure or modify the settings of an alert.
3. *Send Test Alert* is used to check if the alerts have been set and sent out correctly.
4. Click on <Delete> to delete an alert.
5. Click on the <Help> tab to display the Help menu. This menu shows you how to set up or modify an alert.

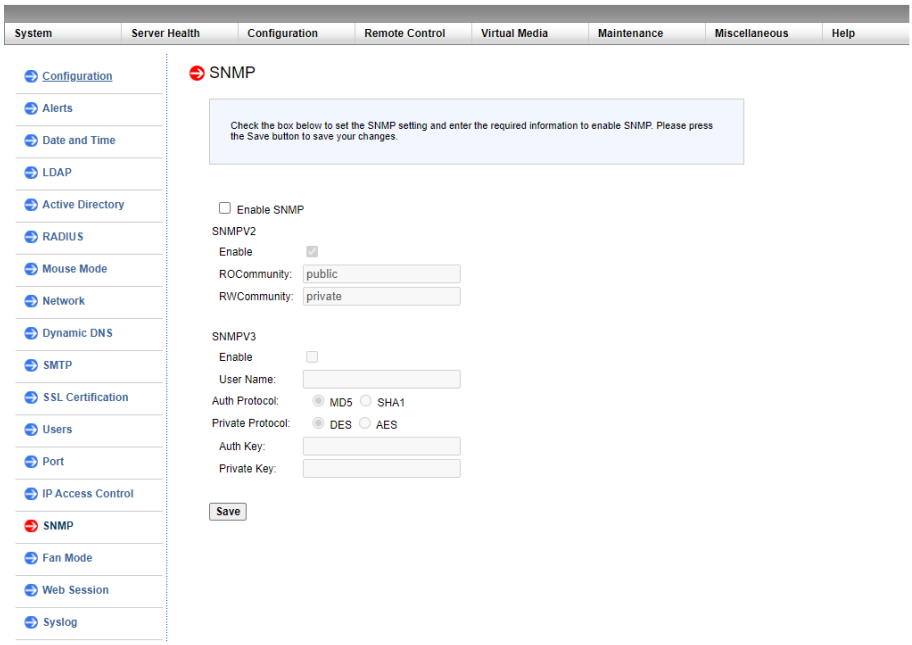


Follow the steps below to setup an alert.

1. Select *Alerts* from the window on the left. Highlight the alert and select *Modify*.
2. Select *Event Severity*.
3. Enter the destination IP address to use SNMP.
4. Enter the email address you wish the send the alert to, then configure the SMTP settings
5. Enter the subject line of the alert.
6. Enter a message for the alert.

After completing the steps above, Click on <Save> to save the settings

SNMP Configuration



1. Check the box to enable the SNMP. Once it is enabled, enter information in the fields below.
2. SNMP Version: Select SNMPV2 or SNMPV3.
3. SNMPV2: If this options is selected, enter a password for ROCommunity and RWCommunity.
4. SNMPV3: If this option is selected, enter information in the fields below: Enter a username
    - Select the Authentication Protocol
    - Select the Private Protocol
    - Enter the Authentication Key
    - Enter the Private key
5. Click <Save> to save the settings.
6. Click the <Help> tab to display the Help menu. The menu includes an explanation of all the options on this page.

CONTACT INFORMATION

For further assistance, contact technical support

Please be prepared to provide the following information: Serial Number (S/N), product name, model number, and a brief description of the issue.

Technical Support
Support@fibrenetix.com

EUROPE & AMERICAS

Fibrenetix
Langebjerg 23B
4000 Roskilde
DENMARK
P. + 45 70 22 10 16
sales@fibrenetix.com
support@fibrenetix.com

MIDDLE EAST

Fibrenetix Middle East
www.fibrenetix.com
sales@fibrenetix.com