



RS9 Management Access

- RAID Controller
- Server





Copyright © 2021 Fibrenetix Aps or its subsidiaries. All rights reserved.

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	4
Web Browser Management	5
Event Log	5
E-mail Alert	6
SNMP Configuration	6
Raid Controller management Access via LAN	7
Fibrenetix RS9 Server Administration	7
Configuring SNMP Services on Windows Server	7
Installing and Configuring SuperDoctor5	8
Web Based Server Monitoring	9
Alert Configuration	
Report	
IPMI LAN Management	
Configuring BIOS	
Accessing the Server Using the Browser	
Alert Configuration	
SNMP Configuration	
CONTACT INFORMATION	



٠



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



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

- Username: "admin"
- > Password: "0000

admin	
••••	
Remember my credentials	
OK	Cancel
UN	Concer

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

🖏 Services					- 0	×
File Action View	Help					
⇐ ➡ 🖬 🗎	3 📑 🛛 🖬 🕨 🔲 🖬 🕨					
Services (Local)	Services (Local)					
	ArcHttpProxyServer	Name	Description	Status	Startup Type	Log ^
	Stop the service Restan the service	ActiveX Installer (AxInstSV) Alloyn Router Service App Readiness App Readiness Application Identity Application Identity Application Information Application Anagement Application Management Adv Deployment Service (ArchitpProvServet Auto Time Zone Updater Background Intelligent Tran	Provides Us Routes AllJo Gets apps re Determines Facilitates t Provides su Provides inf Automatica Transfers fil	Running Running Running	Manual Manual (Trig Manual (Trig Manual (Trig Manual Manual Automatic Disabled Manual	Loc Loc Loc Loc Loc Loc Loc Loc Loc
		🖾 Background Tasks Infrastru	Windows in	Runnina	Automatic	Loc





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.

Modify Pess-Through Disk						
Delete Fess-Through Disk Disk Clone Disk	Stop Auto	Step Auto Refresh				
	• RaidSet Hierarchy					
t Set Disk To Be Falled	RAID Set	Device	1	Volume Set(Px/Targ.Lun)		
Artivate Failed Diek	Raid Set # 000	Erisio	#1.	ST353-DM-VOL#000(06.18293/00.01		
Identify Enclosure		ÉFLSIO	92.			
) Identify Drive		E#1Sot	43			
yatem Controla		E+15id	64			
System Configuration		EFLSIO	05			
Advanced Carriguration		E#15lot	#6			
ISCSI Configuration		E#1Sot	#7			
Etherliet Configuration		E#1900	00			
Alert By Hell Configuration						
SNHP Configuration	-					
NTP Configuration	. Enclosure#1	: SAS RATD Subsyst	em V1.0			
View Events/Nube Besper	Device	Usage	Capacity	Madel		
Generate Test Event	Slot#1[1A]	Raid Set # 000	4000.855	TOSH05A MD03AC4400V		
Modify Reported	Slot#2(19)	Rald Set # 800	4000.555	TOSHIBA MD03AC4400V		
Linutate Elminate	Slot#3(D)	Raid Set # 800	4000.055	TOSPUBA MD03AC6400V		
Shutdown Controller	Sidt#4(F)	Rald Lat # 000	4000.008	TOSHIBA NEICIACA400V		
Restart Controller	SILEPSICE	Raid Set # 000	4000.808	TOSHUBA MD03AC4400V		
formetion	Siet+6(17)	Raid Set + 000	4000.0GB	TOSHIBA MD03AC4400V		
RAID Set Hierarchy	Skit#7(10)	Rett Set # 000	4000.008	TOSHOBA HIDOJACA400V		
SAS Chip Information	Slot #8(11)	Raid Sat # 000	4000.858	TOSHIBA MINISACA400V		
System Information	Glot#9(8)	Free	4000 BGB	TOSHORA HIDOJACA400V		
Hardware Monitor	Sigt#10(18)	Free	4000.835	TOSHORA MD03AC4400V		
0.000.000.00000000000000000000000000000				1 T T T T T T T T T T T T T T T T T T T		
CONTRACTOR OF T	Sigt#11(E)	Frus	4000.005	TOGHOBA MEDDACA400V		
	Slot#11(E) Slot#12(12)	Frus Frus	4000.005	TOSHOBA MD03ACA400V TOSHIBA MD03ACA400V		

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"

	CONFIGURATIO	ON MANAGER		
Erase Failed Disk				
RevertSP	System Events Info	mation		
🖻 😋 Physical Drives	Time	Device	Event Type	Elapse Time
Create Pass-Through Disk	2018-03-14 08:45:40	ST350-DM-VOL#000	Start Initialize	
Delete Pass-Through Disk	2018-03-14 08:45:38	ST350-DM-VOL#000	Create Volume	
Clope Disk	2018-03-14 08:27:23	192.168.008.105	HTTP Log In	
Abort Cloning	2018-03-14 07:59:26	Raid Set # 000	Create RaidSet	
Set Disk To Be Failed	2018-03-14 07:59:11	Raid Set # 000	Delete RaidSet	
Activate Failed Disk	2018-03-14 07:50:08	Raid Set # 000	Create RaidSet	
Identify Enclosure	2018-03-14 07:49:52	Raid Set # 000	Delete RaidSet	
Lantify Drive	2018-03-14 07:49:20	Raid Set # 000	Create RaidSet	
System Controls	2018-03-14 07:48:59	Raid Set # 000	Delete RaidSet	
System Configuration	2018-03-14 07:42:08	Raid Set # 000	Create RaidSet	
Hdd Power Management	2018-03-14 07:28:31	Raid Set # 000	Delete RaidSet	
- iSCSI Configuration	2018-03-14 07:28:09	H/W Monitor	Raid Powered On	
EtherNet Configuration	2018-03-14 07:27:43	192.168.008.105	HTTP Log In	
- Alert By Mail Configuration	2018-03-14 07:09:44	H/W Monitor	Raid Powered On	
SNMP Configuration	2018-03-14 07:09:37	192.168.008.105	HTTP Log In	
NTP Configuration	2018-03-14 07:00:27	192.168.008.105	HTTP Log In	
View Events/Mute Beeper	2018-03-14 06:59:49	192.168.008.100	HTTP Log In	
Generate Test Event Clear Event Buffer	2018-03-14 06:58:24	192.168.001.100	HTTP Log In	
Modify Password	2018-03-14 06:53:52	192.168.001.100	HTTP Log In	
Upgrade Firmware	2018-03-14 06:37:38	E#1 Power#2	Recovered	
Shutdown Controller	2018-03-14 06:37:38	E#1 FAN#4	Recovered	
Restart Controller	2018-03-14 06:37:38	E#1 FAN#3	Recovered	
🗄 🗀 Information	2018-03-14 06:37:06	E#1 Power#2	Failed	
	2018-03-14 06:37:06	E#1 FAN#4	Failed	
http://102.168.8.250/out0.htm	2018-03-14 06:37:06	E#1 FAN#3	Failed	
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2018-03-14 06:27:04	F#1 Power#2	Recovered	





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

Raid System Console	SMTP Server Configuration				
8 🗀 Quick Function	SMTP Server IP Address	0.0.0			
E Ca Volume Set Functions	Mail Address Configurations				
e 📋 Physical Drives	Sender Name :	Mail Address :			
System Configuration	Account :	Password :			
- Advanced Configuration	Event Notification Configurations				
EtherNet Configuration	MaiTo Name1 :	Mail Address :			
 Alert By Mail Configuration 	C Disable Event Notification	No Event Notification Will Be Sent			
SNMP Configuration NTP Configuration	C Urgent Error Notification	Send Only Urgent Event			
- View Events/Mute Beeper	C Serious Error Notification	Send Urgent And Serious Event			
Generate Test Event Clear Event Buffer	C Warning Error Notification	Send Orgent, Serious And Warning Event			
Modify Password	C Information Notification	Send All Event			
Upgrade Firmware	Notification For No Event	Notify User If No Event Occurs Within 24 Hours			
Shutdown Controller Restart Controller	MailTo Name2 :	Mail Address :			
🗈 🗀 Information	Disable Event Notification	No Event Notification Will Be Sent			
	C Urgent Error Notification	Send Only Urgent Event			
	C Serious Error Notification	Send Urgent And Serious Event			
	C Warning Error Notification	Send Urgent, Serious And Warning Event			
	C Information Notification	Send All Event			
	Notification For No Event	Notify User If No Event Occurs Within 24 Hours			
	MailTo NameJ :	Mail Address :			
	C Disable Event Notification	No Event Notification Will Be Sent			
	C Urgent Error Notification	Send Only Urgent Event			
	C Serious Error Notification	Send Urgent And Serious Event			
	C Warning Error Notification	Send Urgent, Serious And Warning Event			
	C Information Notification	Send All Event			
	Notification For No Event	Notify User If No Event Occurs Within 24 Hours			
	MalTo Name4 :	Mail Address :			
	G Disable Event Notification	No Event Notification Will Be Sent			
	C Urgent Error Notification	Send Only Urgent Event			
	C Serious Error Notification	Send Urgent And Serious Event			
	C Warning Error Notification	Send Urgent, Serious And Warning Event			
	C Information Notification	Send All Event			
	Notification For No Event	Notify User If No Event Occurs Within 24 Hours			

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.

pari all'ucce all	58.0.26:82					
Paid System Console	fibrenetix Storage Server CONFIGURATION MANAGER	www.fibrenetyx.com				
Yolume Set Functions						
Physical Drives	 SNMP Trap Configurations 					
System Controls	SNMP Trap IP Address #1	0	. 0 . 0 .	. 0	Port#	162
System Configuration	SNMP Trap IP Address #2	0	. 0 . 0 .	. 0	Port#	162
- Advanced Configuration	SNMP Trap IP Address #3	0	. 0 . 0 .	. 0	Port#	162
Hid Power Management	SNMP System Configurations					
EtherNet Configuration	Community					
- SNMP Contouration	sysContact.0					
NTP Configuration	sysName.0					
-D view Events/Mute beeper	sysLocation.0					
- Generate Test Event	SNMP Trap Notification Configurations					
Clear Event Buffer	Disable SNMP Trap		No SNMP Tra	p Will Be Sent		
Modify Password	O Urgent Error Notification		Send Only U	rgent Event		
Opgrade Himware	O Serious Error Notification		Send Urgent	And Serious Event		
D Restart Controller	O Warning Error Notification		Send Urgent	, Serious And Warning Event		
Ca Information	O Information Notification		Send All Eve	nt		
	SNMP Through PCI Inband		Ethernet SN	MP Is Disabled		
	Submit Reset					



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.

← → C ▲ Not secure 192.1	67.99.136 :82	0 4 5
	fibrenetix storage Server CONFIGURATION MANAGER www.fibrenetix.com	
open all close all		
Raid System Console	Ether Net Configurations	
	DHCP Function	Disabled V
🗉 🧰 RAID Set Functions	Local IP Address (Used If DHCP Disabled)	192 . 168 . 200 . 250
Volume Set Functions	Gateway IP Address (Used If DHCP Disabled)	192 . 168 . 200 . 10
	Subnet Mask (Used If DHCP Disabled)	255 .255 .255 .0
System Controls	HTTP Port Number (71688191 Is Reserved)	80
	Telnet Port Number (71688191 Is Reserved)	23
Hdd Power Management	SMTP Port Number (7168, 8191 Is Reserved)	25
EtherNet Configuration	Current ID Address	192 168 200 250
Alert By Mail Configuration	Current Gateway IP Address	192.168.200.10
SNMP Configuration	Current Subnet Mask	255.255.255.0
View Events/Mute Beeper	Ether Net MAC Address	00.1B.4D.11.63.23
Generate Test Event		
	Confirm The Operation	
- Modify Password	Submit Reset	
Upgrade Firmware		

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.





Server Manager		- 0
🕘 🔹 Server Mar	nager • Dashboard	- 🗇 🏲 Manage Tools View Hel
Dashboard	WELCOME TO SERVER MANAGER	
Local Servers All Servers File and Storage Services D	(1) Configure this local ser	ver
	2 Add roles and features	
	3 Add other servers to man	age
	4 Create a server group	
	S Connect this server to close	ad services
	LEARN MORE	Hide
Add Roles and Features Wizard		- 🗆 X
Installation Type	Features	Description
Server Selection Server Roles Features Confirmation Results	Remote Assistance Remote Differential Compression Remote Server Administration Tools (2 of 41 instal RPC over HTTP Proxy Setup and Boot Event Collection Simple TCP/IP Services SMB 1.0/CIFS File Sharing Support (Installed) SMB Bandwidth Limit SMTP Server SMB Service (0 of 1 installed) SMD Service (0 of 1 installed) SMD VMI Provder Terlnet Client TFD C Lient TFD C Lient WebDAV Redirector Windows Defender Framework Windows Defender Framework Windows Indentity Foundation 3.5 Windows Indentity Foundation 3.5	SNMP Windows Management Instrumentation (WMI) Provider enables WMI client scripts and applications to access SNMP information. Clients can use WMI C+ + interfaces and scripting objects to communicate with network devices that use the SNMP protocol and can receive SNMP traps as WMI events.
	Imili Windows PowerShell (2 of 5 installed) ✓ ✓	> Install Cancel

- 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

depend on it will fail to start.	Smart Card Device Enumera	Creates soft Running Allows the s	Manual (Trig Manual	Loc
	Statut Structure Shall P Trap Source Potention Special Administration Con Spot Venter State Repository Service State Repository Service State Repository Service State Repository Service	Fini Start Rec Stop Alli Pause Ver Resume Dis Restart Pro Las All Tasks Pro Refresh	nual iomatic (D., nual nual (Trig., abled nual nual nual nual (Trig.,	Loc Net Loc Loc Loc Loc
Extended / Standard /		Properties		

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.

	Setup ports
 Introduction License Agreement Choose an install folder Choose a Java VM Check SNMP Service Seturn a key store 	SuperDoctor 5 supports three connection modes: plain text with allowed IP, anonymous SSL connection with allowed IP, and SSL connection with a public key infrastructure. You can configure the port numbers of the three modes.
 Setup ports Configure web and tray Pre-Installation summary Installing Install Complete 	Mode A. Non-SSL Port 5333 Mode B. SSL Port 5666 Mode C. Keypair Port 5999

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.

	Configure web and tray
 Introduction License Agreement Choose an install folder Choose a Java VM Check SNMP Service Setup a key store 	The SuperDoctor 5 contains a pluggable web server module and a system tray component that can be enabled or disabled. Note that you can also configure the detailed web settings of the SuperDoctor 5 Web If it is enabled.
 Setup ports Configure web and tray Pre-Installation summary Installing 	Do you want to enable the SuperDoctor 5 Web? Yes O No HTTPS Port 8444
O Install Complete	Enter login user name and password: User Name admin Password 0000l
	Do you want to enable the SuperDoctor 5 Tray? Yes ONo

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
- 9 RS9 Management Access_R2 User Guide



localhost:8444/SuperDoctor5/login

User Name:	
admin	
Password:	
••••	
••••	

Par Speed	Charles
	Pit So
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Rite

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 to an OK state to an OK state to a non-OK state to an OK state to a non-OK state to a non-OK state to a non-OK state to an OK state to a non-OK state to a non-OK state to 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.

10 – RS9 Management Access_R2 - User Guide





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

Alert Configuration > Manitored Item > Account Setting > Flash BIOS >	Alert Configuration Enable polling					
	Polling Interval* 3 Seconds. (Minimal value is 3)					
	Log (Log monitored item readings.) Max Backup Index* 5 backup files to keep around.					
	E-Mail Alert (In order to send E-Mail alerts to the administrator, the system must be connected to a LAN.) Recipients* (Multiple values are separated by a consolid server* Port* 25 Sender E-Mail Box* Connection Security* None SSL StartTLS My E-Mail Server requires authentication Sender Account Name*					
	Sender Password* SNMP Trap (SNMP trap notification.) SNMP Trap Receivers* (Format: IPv4:port or [IPv6]:port and multiple values are separated by a comma)					
	System Tray Popup Alert (Desktop popup notification)					

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.





🔶 🤿 📷 🗊 🖻 🕞 📓 t	SNMP Service Properties (Local Computer)	×		
C. Services (Local) Services (Local) SNMP Services	General Log On Recovery Agent Traps Security Dependencies	Status	Startup Type	Log "
Stop the ser Restart the r	Accepted community names Community Pagets	Running	Manual Manual Automatic Manual (Trig.,	Loc Loc Loc Loc
Description Enables Sim Manageme requests to	и и в	Running	Manual (Trig Manual (Trig Automatic (T	Loc Loc Loc
computer. If the compute process SNM is disabled, a	Add Edit Remove	Running	Disabled Automatic Manual (Trig	Loc Loc Loc
depend on i	e (Accept SNMP packets from these hosts	Running	Manual (Trig Manual	Loc
	Add Edt Remove	Running	Automatic Manual Automatic (D Manual Manual (Trig Disabled	Loc Net Loc Loc Loc
	OV Count Inclu	Running	Manual Manual	Lec Lec

• 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.

Cax.	Administrator: Command Prompt	×
C:\Users\Administrator>sc	query snmp	^
SENTICE_MILE SIMP TYPE STATE WIN32_EXIT_CODE SERVICE_EXIT_CODE CHECKPOINT WAIT_HINT	: 10 WIN32_OWN_PROCESS : 4 RUNNING	
C:\Users\Administrator>_		\checkmark

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 Key to Enter the UEFI BIOS
- 2. During the system bootup, press the 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].

≹≹≹**#¥≹¥¥¥¥¥¥¥¥¥¥¥¥¥ Configure IPV4 support		BIOS will set below setting to IPMI in next BOOT
каникания selection IPMI LAN Selection IPMI Network Link Status Current Configuration Address sou Station IP address	Failover Dedicated LAN DROP 172.31.33.291	
Subnet mask Station MAC address Jateway IP address VLAN Yes	255.255.0.0 pdate IPMI LAN Configura	e lent Scheen
Jodate IPMI LAN Configuration		elect Item Enter: Select +/-: Change Opt.
		Fi: General Help

13 - RS9 Management Access_R2 - User Guide





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.

BMC Net	twork Configuration	
мекккналамамамамикккк Configure IPV4 support жекккналамамамикккк		Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will poit modify any BMC permock
IPHI LAN Selection IPHI Network Link Status Current Configuration Address sour Station IP address Submet mask Station MAC address Gateway IP address VLAN	Failover Dedicated LAN DHCP 172.31.33.231 255.255.0.0 0c-c4-7a-d5-57-c1 172.31.0.1 Disabled	parameters during BIOS phase
Update IFMI LAN Configuration IFMI LAN Selection VLAN Configuration Address source Station IP address Subnet wesk Bateway IP address	[Yes] [Failoven] [Disabled] [Static] 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0	<pre>##: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</pre>

Aptio Setup Utility -	Copyright (C) 2016 An
BMC Ne	twork Configuration
BMC Network Configuration	
IPMI LAN Selection	Failover
Current Configuration Address sour	DHCP
Station IP address	0.0.0.0
Subnet mask	0.0.0.0
Station MAC address	ac-1f-6b-89-78-4c
Router IP address	0.0.0.0
VLAN	Disabled
Update IPMI LAN Configuration	[Yes]
IPMI LAN Selection	[Failover]
VLAN	[Disabled]
Configuration Address source	[Static]
Station IP address	192.168.5.51
Subnet mask	255.255.255.0
Router IP address	0.0.0.0

14 - RS9 Management Access_R2 - User Guide





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.

Ple	Please Login						
Username							
Password							
	login						

• 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.

					Host Identific Server: User:	ation 192.168.005.051 ADMIN (A	Administrator)	
System	Server Health	Configuration	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help	
🔿 System	\ominus Sys	Alerts Date and Time LDAP						
FRU Reading	Firmware	Active Directory RADIUS	IP Address: 19 BMC MAC Address	2.168.005.051				
Hardware Inform	Instion EIOS Pui EIOS Pui Redish V CPLD Ve	Mouse Mode Network Dynamic DNS SMTP SSL Certification Users Port PrAccess Control PrAccess Control PrAccess Control PrAccess Control SNMP Vian Sesson Systog	System LAN1 System LAN2 System LAN3 System LAN4 noole Preview eview image	MAC address ac 1160 82 MAC address ac 1160 82 MAC address ac 1160 82 MAC address ac 1160 82	2584 2586 2588 2588 2587			
		1-04						

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

System	Server Health	Configurat	ion	Remote Control	Virtual Media	Maintenance	Miscellaneous	Help
Configuration	9	SNMP						
Alerts								
Date and Time		the Save button	to save you	the SNMP setting and ente ir changes.	er the required information to	o enable SNMP. Please pres	55	
🔿 LDAP								
Active Directory		Enable SNMF	, ,					
RADIUS		SNMPV2	_					
I Mouse Mode		Enable ROCommunity:	public					
Network		RWCommunity:	private					
Dynamic DNS		SNMPV3						
SMTP		Enable						
SSL Certification	1	User Name: Auth Protocol:	MD5	S O SHA1				
🔿 Users		Private Protocol:	DES	AES				
Port		Auth Key: Private Key:						
IP Access Control	ol							
SNMP		Save						
🔿 Fan Mode								
Web Session								
Syslog								

- 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
 - o Select the Authentication Protocol
 - o Select the Private Protocol
 - o Enter the Authentication Key
 - o 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 <u>Support@fibrenetix.com</u>

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