# Sonarman User's Guide

Version 1.0

DevelUp Japan Corporation

<<Contents>>

○ Overview P. 2

○ Product features P. 3

○ Operation instructions P. 4

○ Product specification P. 7

○ FAQ P. 8

## Introduction

Sonarman can be continuously capture network packet.

Sonarman is useful tool in following cases.

- Resolving network problem that difficult to reproduce
- Make efficient of troubleshooting
- Complement the log function
- Enable to save evidence

## Description

Sonarman was developed for the purpose of dealing with packet as network evidence to simple.

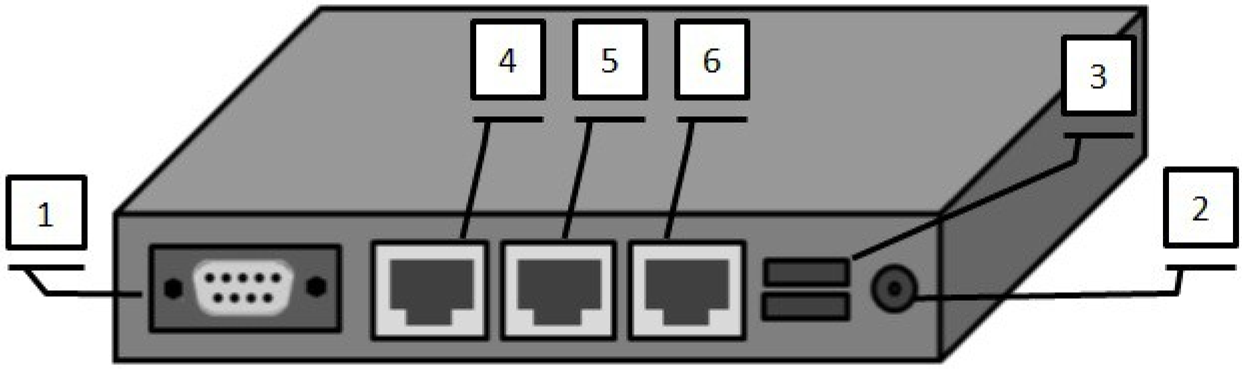
Sonarman works with syslog by swatch.

This software can save packet depending on syslog messages.

You can save evidence surely when a problem happened.

I hope Sonarman will reduce the trouble of system administrators.

## Identifying parts



1 Serial port

BaudRate is 115200

2 Power

DC 12V 0.5-1A 2.5mm

3 USB

4 Gigabit Ethenet eth0

For control (WebUI, ssh, VPN support)

5 Gigabit Ethenet eth1

For packet capture

6 Gigabit Ethenet eth2

For packet capture

Ethernet Left LED (green) indicates activity.

Right LED indicates connection mode.

## Deploy

Refer to SetupGuide.md

## How to start

Connect a power plug to Sonarman.

By default, eth0 get IP address by DHCP client.

Confirm IP address from serial console.

Login as sonarman/sonarman

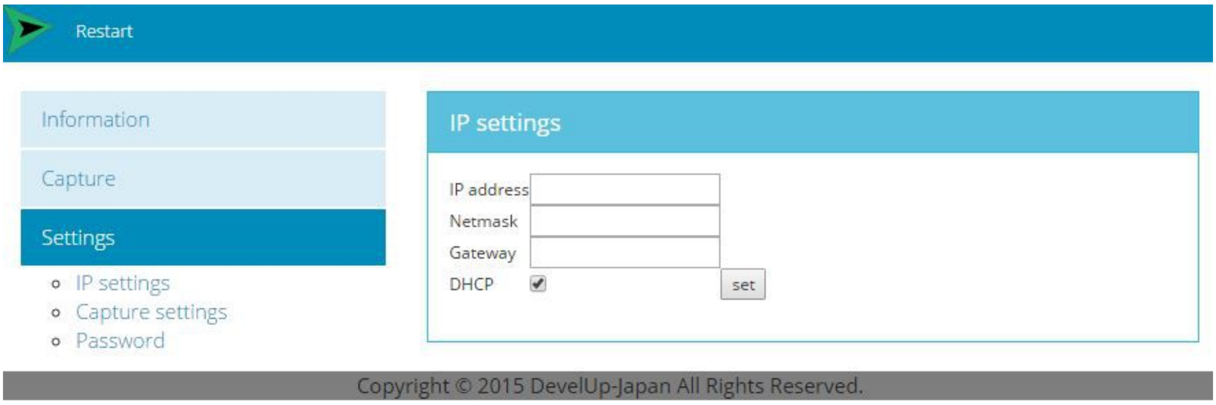
## WebGUI

Access to http://ipaddress/

Login as admin/pass

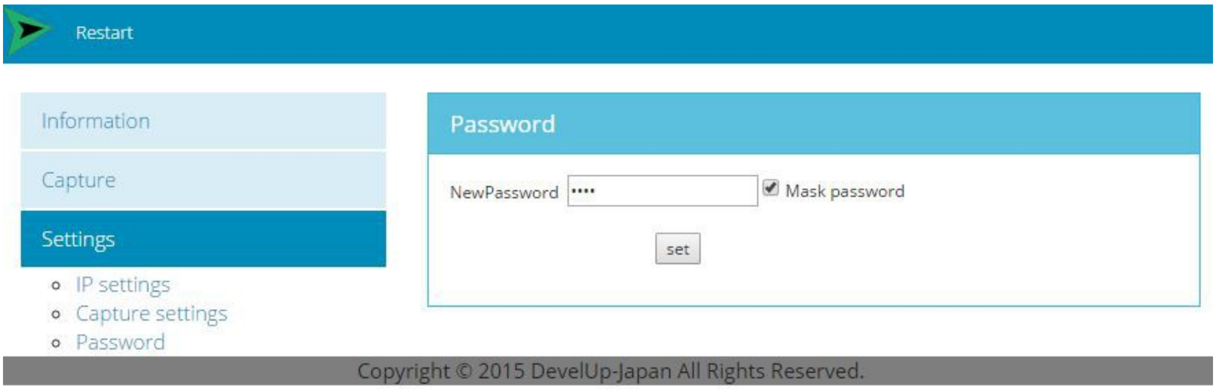
## Network configuration

You can configure eth0 interface (IPv4)



## Change password

You can change password.



Password

NewPassword •••• ☑ Mask password

## Configure capture settings

The size value is calculated in KB

The filesize must be between 1M and 2G

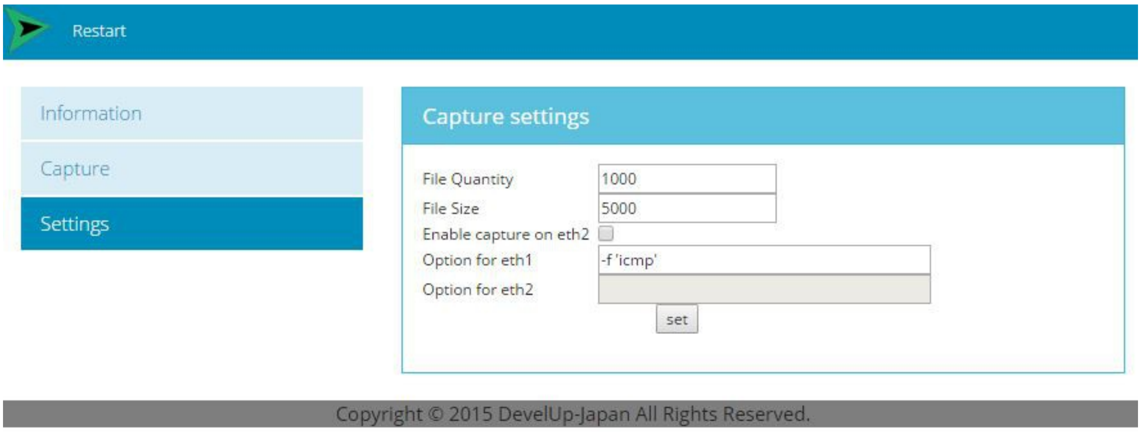
the quantity value must be between 10 and 100000

The total value of filesize and quantity is limited to 80% of a maximum disk size.

Capture option is used as following.

Ex) -f 'ip.addr==192.168.1.1 && http'

You can input any tshark option.



Capture settings

| | |
|---|---|
| File Quantity | 1000 |
| File Size | 5000 |
| Enable capture on eth2 | □ |
| Option for eth1 | -f 'icmp' |
| Option for eth2 | |

## VPN Support

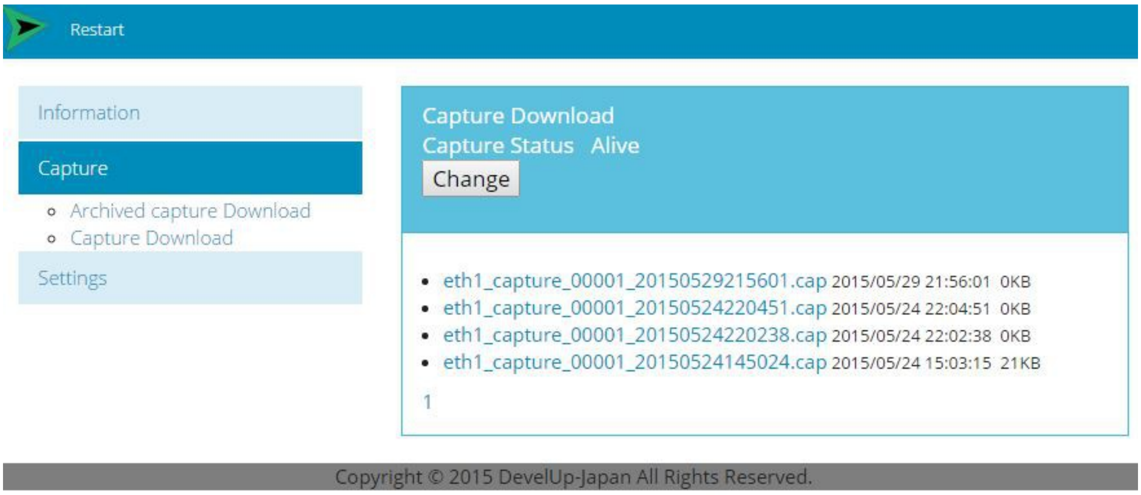
This function is not supported in open source edition.

## Capture file download

You can download ring buffer capture.

The capture files are over written with time.

If you want to change the current capture file, press "Change" button.



Capture Download
Capture Status Alive

- eth1_capture_00001_20150529215601.cap 2015/05/29 21:56:01 0KB
- eth1_capture_00001_20150524220451.cap 2015/05/24 22:04:51 0KB
- eth1_capture_00001_20150524220238.cap 2015/05/24 22:02:38 0KB
- eth1_capture_00001_20150524145024.cap 2015/05/24 15:03:15 21KB

1

Copyright © 2015 DevelUp-Japan All Rights Reserved.

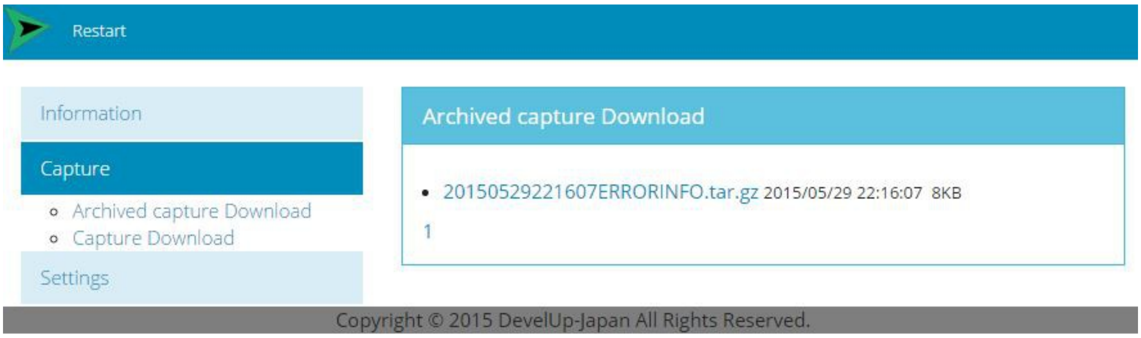
## Archived capture file download

You can download saved and archived capture by syslog message.

You can save 2 capture files (current and latest) each interface by syslog message.

The syslog message that trigger of saving capture is "ERRORINFO".

If you want to change the trigger word, edit /home/sonarman/shells/swatchrc.



Archived capture Download

- 20150529221607ERRORINFO.tar.gz 2015/05/29 22:16:07 8KB

1

Copyright © 2015 DevelUp-Japan All Rights Reserved.

# Product specification

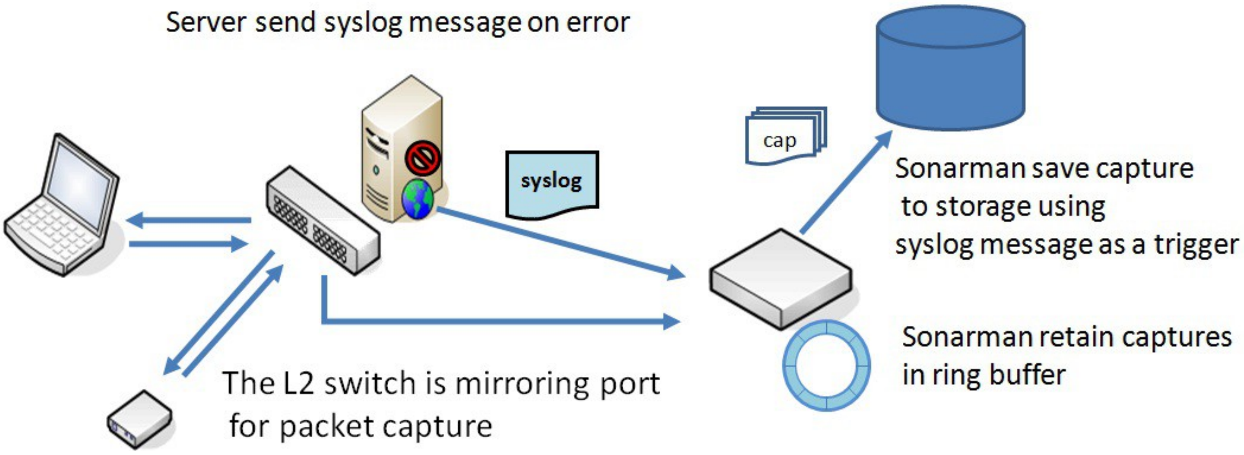
| HW specification | |
|---|---|
| Model Number | SM−001 (SMV−001 is virtual appliance edition) |
| Size (Height X Width X Depth cm) | 3.0X 16.8 X 15.7 |
| Interface | Ethernet ×3, serial port (console) ×1, USB×2 |
| Ethernet standard | IEEE 802.3u (10/100Mbps) IEEE 802.3ab (1000Mbps ) |
| Memory | 2G |
| AC Power | 12V DC, 1A, 2.5 mm |
| Storage | SSD 128Gbyte（extendable） |
| CPU | AMD G−T40E (1GHz 2core x64 support) |

# FAQ

## How to connect Sonarman to a network?

Sonarman is expected to use with port mirroring

If you want to hold capture as much as you can in ring buffer, you can use filter option.


Server send syslog message on error
syslog
cap
Sonarman save capture to storage using syslog message as a trigger
Sonarman retain captures in ring buffer
The L2 switch is mirroring port for packet capture