Silicom Connectivity Solution
14 Atir Yeda St.
Kfar-Sava 4464323, Israel
Fax: (972)-9-7651977

Silicom uBMC
User Guide

Table of Contents

Table of Figures

1. Introduction

The Silicom uBMC module is an IPMI compatible basic Board Management Controller for Silicom's vE-CPE edge networking devices.
The uBMC provides a way to securely manage the vE-CPE devices that will sit in customer premises over the internet. It combines the feature of traditional IPMI, and also the secure management IPSec channel for all communications and modern NETCONF management interface.

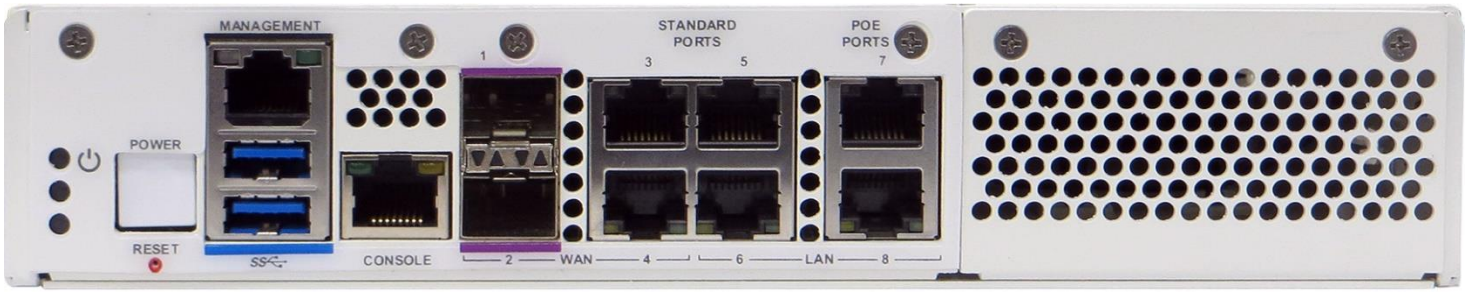
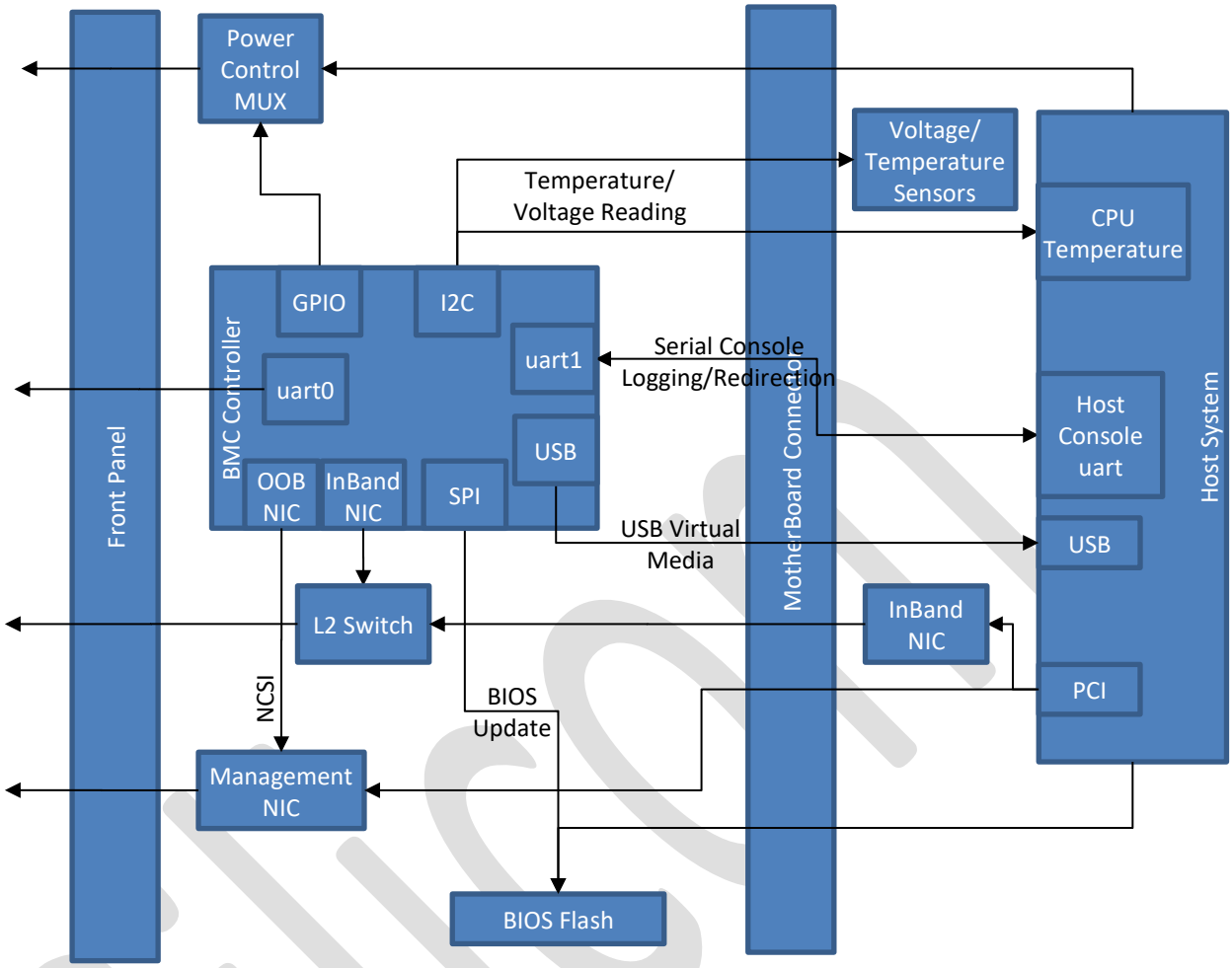


Figure 1. vE-CPE 1U Unit front panel

The uBMC module is a front I/O module that can be inserted into the vE-CPE systems.
There are 3 flavours of uBMC modules available for different vE-CPE systems.

1.1 uBMC Block Diagram



The following table explains the items in a Silicom vE-CPE shipment package.

P/N	Item	Description
80500-0150-G05	1 x Kit	vE-CPE, Desktop XS Module, Empty
25700-0021-G00	1 x PoE Power supply	POWER SUPPLY: EXT DESKTOP, 54V POE, 65W, LATCHI
25700-0017-G00	1 x 12V Power Supply	POWER SUPPLY: EXT DESKTOP, 12V, 60W, LATCHING AT
28300-0001	1 x Power Cord	POWER CORD, AC, 120V, 18AWG, 3COND, M/F, SJT JAC

The following table explains top-level Kit Part Number of the Silicom vE-CPE device with uBMC module.

P/N	Description	Notes:
80500-0150-G05	Shippable Kit: vE-CPE, Desktop XS Module, Empty Right Slot, C3558 (4C), DDR4 8GB ECC, EMMC 64GB, including +12V, +56V Power supplies	Top level – Shippable kit, including packaging, GA

2. Features and Specifications

2.1 List of features

Here's a list of the major features provided by uBMC:

- Hardware monitoring
- IPMI SDR Support
- IPMI SEL Support
- Host BIOS upgrade
- Host power control
- Virtual CDROM
- Serial Console Redirection over LAN
- Advanced Networking support with IPSec and VRF
- Dying Gasp support

2.2 Configuration Methods

The uBMC can be configured through the following methods:

- Simple command line interface (CLI), via a serial communication console port and an Ethernet port using SSH
- Simple Web management interface
- Simple Network Management Protocol (SNMP)
  Note: Not supported in the current release

2.3 Hardware monitoring

The uBMC monitor the following hardware status.

System Fans Speed and health.

System wide power status and voltages.

System wide temperatures include:

- Host CPU temperature
- Host PCB temperature
- System ambient air temperature

Hardware monitoring data can be retrieved via the below interfaces.

CLI – cli interface

Web GUI – Status/System Page

IPMI – ipmitool sensors on the host

2.4 IPMI 2.0 Support

The uBMC is connected to the veCPE host CPU's SMBus controller.

The uBMC support the IPMI 2.0 over SMBus on the connection.

Software running on the host CPU may query the uBMC using the IPMI using the SSIF protocol over the SMBus connection.
Support IPMI 2.0 features include:

- SDR
- Sensors
- SEL
- LAN (read only)

2.5 Host power control

The uBMC can support host system power control. It can report the following status.
CPU S3 - Sleep
CPU S4/5 – Hibernation/Power off
It can also control the reset and power off of the system.

2.6 BIOS update

The uBMC can support update of the system BIOS. The BIOS is still upgradable with the standard X86 BIOS update method. The uBMC however provide an alternative way for the updating the BIOS, even when there's no OS running.

2.7 Virtual CDRom

The uBMC can map an ISO file to the host system via USB interface. The ISO file will appear as an CDRom to the host system. This can be used to install the OS or provide update to the current system.
The ISO file can be stored on the uBMC storage, the uBMC provides about 4GB of storage space for ISO.
Remote ISO attachment via windows file sharing is also supported.

2.8 Serial over LAN

The serial console of the host system is connected to the uBMC, and uBMC will then bridge the serial console to the front panel.
In that sense, the uBMC and the host shares the front panel serial port. User can use Ctrl+X to switch between the uBMC console and host serial console.
This design allows the uBMC to be able to provide logging of the host serial console. This could be useful in the case of OS problems, kernel debugging, ..etc.
The uBMC also provide host serial console access via SSH based CLI.

2.9 Advanced Networking support with VRF

The uBMC has two network interfaces

- In-Band interface - connected directly to the host switch.
- Out-of-Band Interface – connected as side-band to the i210 management ethernet interface.

The uBMC also support the following Network features.

- DHCP
- IPV4/IPV6
- IPSec
- VRF

2.10 VRF – Virtual Routing and Forwarding

The VRF device combined with ip rules provides the ability to create virtual routing and forwarding domains (aka VRFs, VRF-lite to be specific) in the Linux network stack. One use case is the multi-tenancy problem where each tenant has their own unique routing tables and in the very least need different default gateways.

The uBMC provide the VRF feature as a mean of allowing easier interoperability between the uBMC and various network elements in the complex networking where the vE-CPE is usually deployed.

For more information about the VRF, please have a look at the following document.

https://www.kernel.org/doc/Documentation/networking/vrf.txt

2.11 Dying Gasp

Dying Gasp is a feature for notifying the central management system in the event of power loss.
The uBMC is capable of sending an SNMP alarm when the vE-CPE system loses the power.

2.12 Additional management features

The uBMC also support the following management features.

- Supports remote syslog
- Support RADIUS
- Supports TACACS+
- Supports NTP
- Supports time zone
- Supports multi configuration backup

3. System Management Overview

A user can use a username and password to access the uBMC management interface via COM, SSH or Web.
The initial user name is **is_admin** and the default password is 1qaz2wsX.
The uBMC supports multiple users' login.

The uBMC defines three types of user privileges to restrict user access:

- **Admin:** Full read-write access to all configurations (**BMC Configuration/System/User**);

privileges to add, delete, or modify local users on the uBMC. The initial user account **is_admin** is the only administrator account and no other administrator accounts are allowed to be created. This **is_admin** account cannot be deleted, and the privileges cannot be modified.

- **Normal:** Full read-write access to **BMC Configurations** and read-only access to other configurations **(System/User**)**.**
- **Readonly:** Read-only access to all configurations.

The **Admin** user can change everyone's password.
The **Normal** users and **Readonly** users can just change their own password.

The uBMC supports RADIUS/TACACS+ remote login.
RADIUS and TACACS+ cannot be enabled at the same time.
To enable either, the other needs to be disabled first.

RADIUS users share the same privilege level, which can be configured through Web or CLI.

TACACS+ user or user group privilege can be configured on server side by adding a service tag (default is "silc-system", and this can be configured through Web or CLI, but it can't be the system reserved tags such as slip/ppp/arap/shell/tty-daemon/connection/system/firewall.) to tacacs+ server configuration as below:

```
service = silc-system {

    # 1: readonly; 5: normal; 10: admin

    user-privilege = 10

}
```

And TACACS+ user will be assigned Readonly privilege if the service tag is missing in server configuration.

4. Configuration and Usage Guide

4.1 IPMI Usage Guide

No additional configuration is needed on the uBMC itself to use IPMI. However, the host Linux OS may need to install the ipmitool package.

Follow the below procedures to install ipmitool package on a Debian/ubuntu based system.

```
apt-get install ipmitool
```

To load the ipmi ssif driver

```
rmmod i2c_ismt
modprobe i2c_ismt bus_speed=100
modprobe ipmi_devintf
modprobe ipmi_ssif addr=0x42 adapter_name="ubmc" dbg=1
```

Run ipmitool sensor to verify it is working.

```
ipmitool sensor
```

Notes:

- Refer to the IPMI 2.0 standard, and also ipmitool help for how to interact with uBMC via IPMI ssif.
- ipmitool lan is read only.

4.2 Host Power Status and Control

The uBMC can remotely view the power status and control the power of the host vE-CPE system.
In order to view and control the power, connect to the web GUI or the CLI interface.

4.2.1 Reading the host power status

In the CLI interface, use the following command to view power status

```
show bmc state
```

4.2.2 Controlling the host power

In the CLI interface, use the following set of commands

```
bmc host power on
bmc host power off
bmc host power cycle
bmc host power reset
```

4.3 BIOS Update

There are multiple ways of upgrading the host BIOS in a vE-CPE system:

- In the host Linux OS
- In the uBMC GUI/CLI

In this document, we only cover the uBMC method.

Upgrade BIOS in uBMC can be used as a last resort BIOS recovery when the system BIOS fails to load completely.

The uBMC support upgrade from the following file source.

- http/https
- scp/sftp server (with username password authentication over ssh)

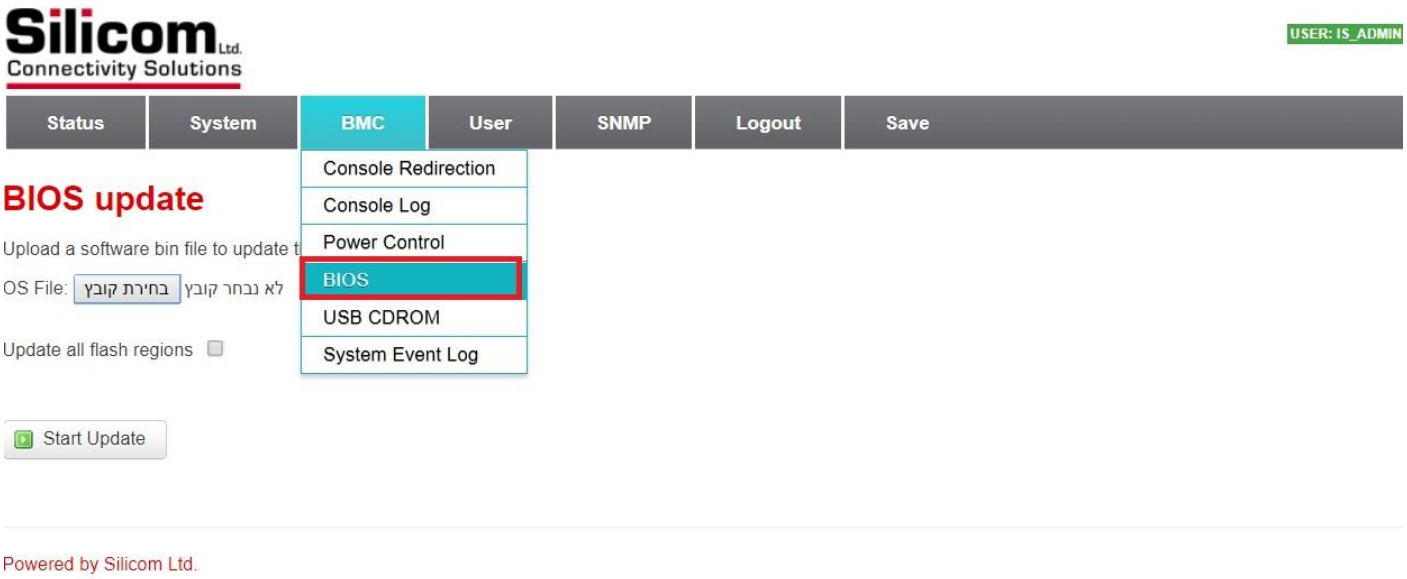
Please obtain system BIOS flash bin file from Silicom support, the system BIOS may differ on different products. Flashing a wrong file may cause the host failing to boot up.

The BIOS flash of the veCPE also contains additional information of the hardware and boot firmware for various on-board devices. Typically, the BIOS update procedure only updates the BIOS sections of the flash, the reset part will be left untouched.

There are certain circumstances when a full update of the BIOS flash is needed, an option is available to allow this. THIS SHOULD ONLY BE ENABLED WHEN INSTRUCTED BY SILICOM SUPPORT TEAM ON A CASE BY CASE BASIS.

Sometimes the files are sent as .gz or tar.gz, the actual BIOS update bin file needs to be extracted first, the size of the BIOS update bin file is exactly 16MB.

4.3.1 Update with GUI



4.3.2 Update with CLI

After boot-up procedure, switch to µBMC Linux console by typing <Ctrl X>
and enter the following credentials ubmc login: **is_admin** / password: **1qaz2wsX.**

Login into "configure" mode and choose the proper option, as an example scp
(see example below):

bmc(config)# bmc bios upgrade file-url scp://xxx@x.x.x.x:/path/file.bin

4.4 Virtual CD ROM

The virtual CD ROM feature provide an easy way to remotely attach an CD ROM ISO file as a USB CD ROM to the vE-CPE host system. This is usually used to install or update the OS.

We support two ways of attaching an ISO file to the host system:

1. Remotely attaching a windows shared ISO file
2. Attaching a previously uploaded ISO

4.4.1 Remotely attaching from windows share

Support windows release:

- Windows 10
- Windows 7
- Windows Server 200x
- Samba server

The windows share must be configured to allow an username and password to allow authentication. Simple share will not work.

4.4.2 Attaching a local ISO

First the ISO files must be uploaded to the uBMC ISO storage space before it can be attached locally as USB CDROM. A local attached ISO image is usually faster than a remote attached image.

Upload through the Web interface is currently not supported, it must be done through CLI with scp or http or https (the uBMC will actually download the file into the uBMC ISO storage)

The uBMC has 4GB of ISO storage room, you can use the web GUI or CLI to manage previously uploaded files.

Attaching ISO can be done with the below commands, or via the web GUI.

4.5 Serial Console Management

4.5.1 Front Panel Serial Port

The front Panel serial port is shared between the host and uBMC.
During the uBMC firmware initialization, the uBMC firmware will take control of the front panel serial port. Immediately after the uBMC firmware is fully initialized, it will switch to front panel serial port to host serial console.

It is possible to switch between uBMC serial console and the host serial console by ctrl+X.

4.5.2 System Boot up sequence

When first connected to the power, the uBMC will start its initialization sequence, during this time the front panel port cannot be used to access the host serial console. If the host CPU is powered on during this period, the BIOS will wait for uBMC to finish initialization before it continues with normal booting. This allows access to the BIOS boot menu through the serial console.

4.5.3 Serial Over LAN

Serial Over LAN is a feature for accessing the host serial console over SSH connection. To use the serial over LAN feature, first an CLI session with SSH connection must be established to the uBMC. See Chapter 3. System Management Overview for how to connect to the uBMC with SSH.

Once connected to the ssh, the following command can be used to connect to the host serial console interactively.

```
bmc console connect
```

Use ctrl+X to quit the console connection and return to the CLI interface.

If the host console uses a different serial settings, the below set of commands can be used to change the default host serial console settings.

```
bmc console speed <value>
bmc console data <value>
bmc console parity <value>
bmc console stop-bits <value>
(no) bmc console hw-flowctrl
(no) bmc console sw-flowctrl
```

The default host serial console setting is

```
Baudrate              : 115200
Data bits             : 8
Stopbits              : 1
Hardware flow control: n
Software flow control: no
```

4.5.4 Host Serial Console Logging

The uBMC has ability to save all host serial console activity into local storage.
This feature could be valuable for host crash post-mortem investigation, boot up monitoring etc.
User can configure the console logging rotation parameters.
However, when being viewed, the log file is being viewed as a consecutive file.
Search and filtering is available when viewing the log in both CLI and GUI.
The following command can be used to view the Host serial console log

```
show bmc console log
show bmc console log filter <filter keyword>
```

When viewing the log with the above command, '/' can be used to search the content. For example, Typing '/abc' will search the log for abc.

4.6 Advanced Networking Management

uBMC has two Ethernet ports:
eth0 (INBAND) – connected to the on-board switch.
eth1 (OOB) – connected to the sideband of the front panel management port.

4.6.1 Configuring Addresses

4.6.1.1 Configuring DHCP

Below is an example for configuring DHCP for interface eth0. The first two commands is to register the hostname to the DHCP server. Some DHCP server can bind the registered name to DNS records.

```
name <new host name for the server>
management interface eth0 dhcp-sendname
management interface eth0 ipv4 dhcp
management interface eth0 ipv6 dhcp
```

4.6.1.2 Configuring Static Addresses

Below is an example for configuring Static Address for interface eth0. The first two commands are to Configure IPv4 address. The last two commands are intended to configure IPv6 address.

```
management interface eth0 ipv4 ip 192.168.1.100
management interface eth0 ipv4 prefixlen 24
management interface eth0 ipv6 ip <ipv6 address>
management interface eth0 ipv6 ip prefixlen <0-128>
```

4.6.2 IN-BAND Management interface Eth0

The in-band interface eth0 is connected to the on-board switch of the veCPE.
As the connection is on-board, it is always operated at 1Gbps.

4.6.3 Out-Of-Band Management Interface Eth1

The veCPE host has a management ethernet front panel port, it is based on an Intel i210 Ethernet controller. The eth1 port of the uBMC is connected to the front panel management port i210 NIC via the side-band connection. The side band connection has a speed of 100Mbps, so the maximum speed for the eth1 is also 100Mbps.
When the host is powered on with the i210 ethernet controller enabled and AUTONEG is enabled, the i210 will try to link up at the highest speed which is 1Gbps. If the link is at 1Gbps, the front panel port link LED will show orange.
When the host is not powered on, or when the i210 ethernet controller is not enabled by the host, the uBMC eth1 will still be able to receive traffic, but the managment port will have link up 100Mbit speed at a maximum. In this case, the front panel port link LED will show green.

4.6.3.1 Default eth1 configuration

In the default configuration eth1 is enabled in the system with DHCP enabled.

4.7 IPSec Configurations

The uBMC IPSEC implementation is based on open source project StrongSWAN. The StrongSWAN IPSec solution does not create a new interface for each connection, instead it operates at the IP layer to provide the secured IPSEC tunnel to applications.
First ipsec needs to be enabled globally.

4.7.1 IPSEC Required information

Setting up IPSec will usually require the below information first.

- Trusted CA
- Local Certification File
- Local AUTH ID
- Remote Certification File
- Remote AUTH ID
- Remote Peer IP

4.7.2 IPSEC Configuration Procedure

Assuming needed files are already on a server 192.168.1.200 with ssh enabled. Then the below commands can be used to upload needed files.
Each upload command may ask for username and password.

4.7.2.1 Create Trust CA

To create the CA, we need to upload the CA certification, and then create the CA with the certification.

```
management ipsec cert MyCACert file-url scp://adam@192.168.1.200:/cert_path/MyCACert.cert
management ipsec ca MyCA cacert MyCACert
```

4.7.2.2 Create secret

The command “management ipsec secret …” is used to create a secret to be used in ipsec authentication. Depending on what the IPSec authentication (from the following) is used, the command line differs, some requires a key to be created/uploaded first.

- PSK
- EAP
- Xauth
- RSA
- ECSDA

For example, to create a secret based on RSA, you will be asked to enter a passphrase

```
management ipsec key MyRSASecretKey file-url scp://192.168.1.200/key_path/MyRSASeretKey
management ipsec secret MYRSASecret rsa key MyRSASecretKey
```

4.7.2.3 Create the connection

We can now create the connection with the root CA and the secret available
For example:

```
# add the private ip on eth1
management address ipsec-pri ip 10.10.10.100 prefixlen 24 interface eth1
# setup ipsec conection
management ipsec connection test
management ipsec connection test compress no
management ipsec connection test dpdaction restart
management ipsec connection test esp aes256-sha2_256-modp1536!
management ipsec connection test ike aes256-sha2_256-modp1536!
management ipsec connection test tries %forever
management ipsec connection test local-ip 17.16.0.100
management ipsec connection test local-src %config
management ipsec connection test local-sub 10.10.10.100/32
management ipsec connection test local-auth psk
management ipsec connection test peer-ip 17.16.0.200
management ipsec connection test peer-src ''
management ipsec connection test peer-sub 10.10.10.0/24
management ipsec connection test peer-auth psk
management ipsec connection test replay-window 0
#setup ipsec secret
management ipsec secret test PSK key PSKkey1
```

4.7.2.4 Testing Created connection

```
# start ipsec service
management ipsec enable
```

4.7.2.4.1 Test with StrongSWAN

Below is a procedure to install a StrongSWAN server on a linux machine

1, install StrongSWAN.

2, modify /etc/strongswan/ipsec.secrets (don't miss the left and right space beside ':'):

: PSK "PSKkey1"

3, modify /etc/strongswan/ipsec.conf to add below:

conn UBMC01

keyexchange=ikev2

left=17.16.0.200

leftauth=psk

leftsubnet=10.10.10.0/24

right=17.16.0.100
rightauth=psk
rightsourceip=%config
ike=aes256-sha2_256-modp1536!
esp=aes256-sha2_256-modp1536!
type=tunnel
compress=no
keyingtries=%forever
replay_window=0
dpdaction=restart
closeaction=restart
auto=start

4, run "strongswan restart"
5, add a virtual ip to another server interface (assume 17.16.0.200 is on dev p5p1, so config an virtual ip on dev p5p2):
#ip addr add dev p5p2 10.10.10.200/24
6, now it should be ok to ping or ssh 10.10.10.100 on the server. If it doesn't work, which might occur after uBMC reboot, please restart ipsec on the server first and then restart ipsec on uBMC (run "no management ipsec enable" then "management ipsec enable").

4.8 VRF – Virtual Routing and Forwarding

4.8.1 Service Separation

VRF allows services to be listened on different routing tables and provides better separation of services. Services supported by VRF on the uBMC currently include:

- ssh
- http/https

The configuration of VRF involves the below 3 commands. The VRF CLI commands has a syntax similar to the linux ip commands.

```
management vrf          - create a VRF routing table
management route        - create new route on VRF routing table
management vrf-process  - bind process to VRF routing table
```

4.8.2 VRF Example

Below is an example for a network setup that utilize the VRF to separate traffic routing into 3 networks.

- In Band
- Out of Band

See the below table for configurations of each network.

VRF Purpose	VRF name	Enslaved interface	admin status	Enslaved IPv4 (IPv6) address	Default gateway	Route table ID	VLAN
Out of band	oob0	eth1	up	DHCP		100	none
In Band	ib0	eth0	up	192.168.0.10/24	eth0	200	none

See below the commands to setup the above VRF example
Here are the CLI commands to setup VRFs on uBMC:

```
# create VRFs
management vrf oob0 table 100
management vrf ib0 table 200

# bind the interfaces to VRFs
management interface eth1 master oob0
management interface eth0 master ib0

#Then here are the CLI commands to configure network processes on VRFs:
#(NOTE! Reboot is required to make theses configurations effective.)
# dying-gasp/ipsec/netconf are running on oob0
management vrf-process dg-oob process dying-gasp vrf oob0 binding-address ''
management vrf-process ipsec-oob process ipsec vrf oob0 binding-address ''
management vrf-process nc-oob process netconf vrf oob0 binding-address ''

# ssh/web need to specify binding-address as service listening address.
management vrf-process ssh-oob process ssh oob0 binding-address 10.10.10.100
management vrf-process ssh-ib process ssh vrf ib0 binding-address 12.80.1.30
management vrf-process web-oob process web oob0 binding-address 10.10.10.100
management vrf-process web-ib process web vrf ib0 binding-address 12.80.1.30
```

4.9 Dying Gasp

The Dying gasp feature send an SNMP alarm to the configured SNMP agent(s).
The feature doesn't need special configuration of itself. But SNMP trap must be enabled, and trap server must be configured.
The trap server can be configured by the following command:

```
snmp host <trap server ip> v2c community public
```

The trap sent will contain the following information:

```
SNMPv2-MIB::snmpTrapOID.0 = OID:
SILICOM-UBMC-MIB::trapDyingGasp
SILICOM-UBMC-MIB::trapModule = STRING: "dyinggasp"
SILICOM-UBMC-MIB::trapEvent = INTEGER: off(7)
```

The uBMC is capable to send the trap to a maximum of 2 SNMP trap servers through eth1 directly, and when ipSEC is enabled, it can only send to a single SNMP trap server.

5. Product Layout

This chapter introduces the front panels and rear panels of the uBMC 1U Unit.

5.1 Front panel

Depending on your order, the uBMC 1U Unit consists of one host system and one or two uBMC modules.

The following figure shows the uBMC 1U Unit front panel (a host system with one uBMC module).

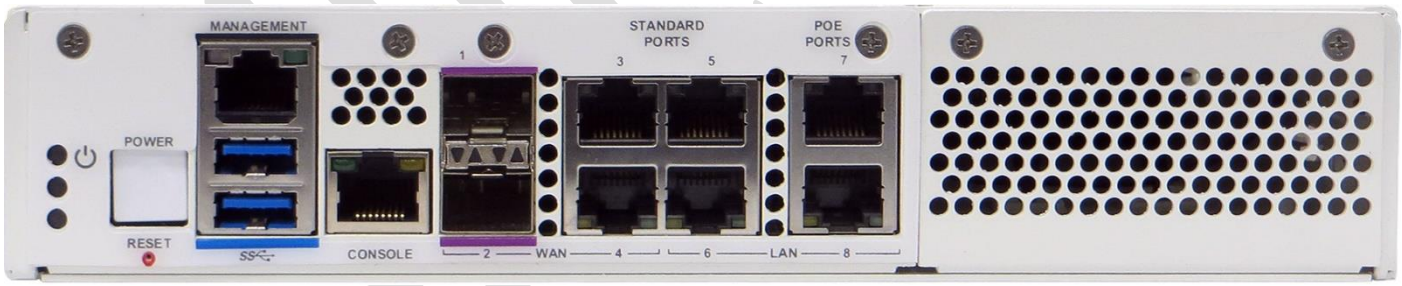


Figure 2. vE-CPE 1U Unit front panel – Host System with one uMBC module

The following figure shows the front panel of the host system. (Power / Reset / Management /Console).

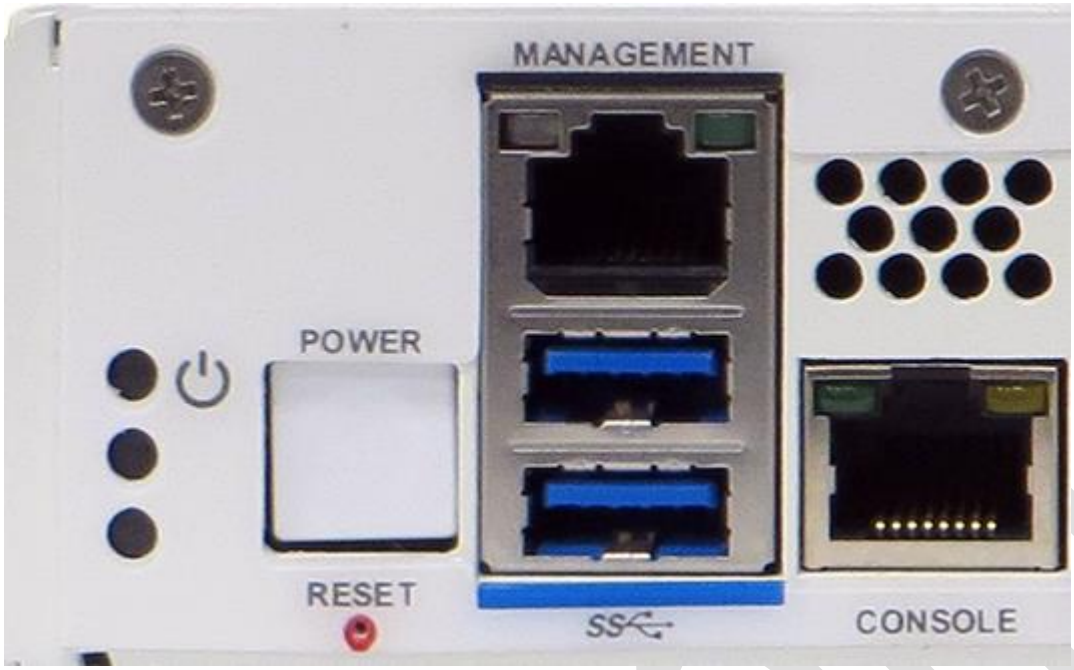


Figure 3. vE-CPE 1U Unit front panel – Power / Reset / Management / Console

The following tables explains the LEDs, Power/Reset button, Management and RS-232 Console port on the front panel of the host system.

Category	Descriptive name	Name on front panel	Description
LEDs	TOP LED (Host system)		Amber(Green+Red) – x86 System is OFF
			Blue – x86 System is ON
	CENTER LED		Connected to I2C Expander.
	BOTTOM LED (uBMC)		Off- uBMC is OFF
			Blue – uBMC is ON (kernel is loaded)
POWER/RESET			
	Power button	Power	Power Up and Shutdown of the veCPE unit
	Reset button	RESET	Reset of the veCPE unit
Management Connectors	Ethernet (OOB port)	Management	Management OOB (Out of Band port) Connected directly to the host CPU through Intel i210 Also support NCSI interface to the uBMC.

	USB1 connector	Management	Can be used for internal/external connections, such as Flash drives or even LTE.
	USB2 connector	Management	Connected to the host CPU and is intended to be used as CD ROM for the Virtual Media.

Management Connector	RS-232 (Serial port)	CONSOLE	The Console Port connected directly to UBMC. After uBMC is up, the user can toggle between uBMC and host by using Ctrl-X

The following figure shows the WAN and LAN ports. (Standard and POE Ports)

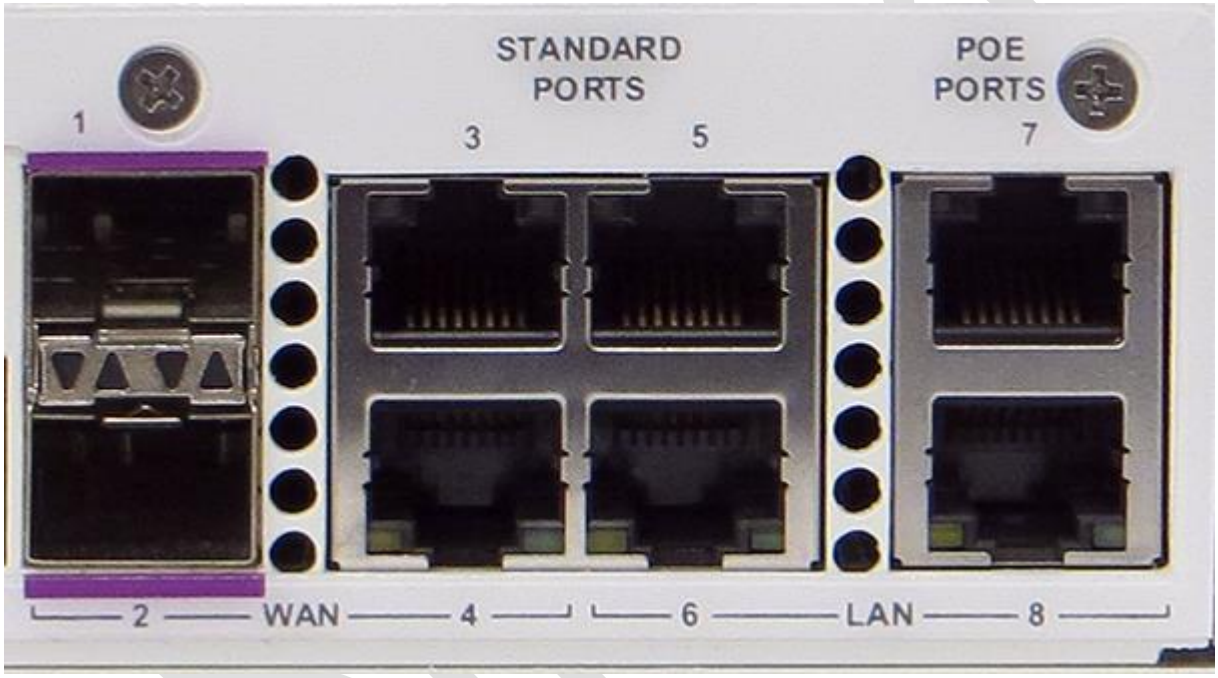


Figure 4. vE-CPE 1U Unit front panel - Standard and POE ports

The following table explains the WAN and LAN ports on the front panel of an uBMC module.

Category	Descriptive name	Name on front panel	Description
WAN (Switch ports)	2x1GbE Fiber ports	WAN	Network 2x1GbE Fiber and 4x1GbE Copper ports based on Marvell switch
	4x1 GbE Copper ports	Standard Ports	
LAN (Switch ports)	2x1 GbE Copper ports	POE Ports	Network 2x1GbE Fiber ports, that are Managed by Microsemi POE (Power Over Ethernet) controller.

5.2 Rear panel

The following figure shows the rear panel of the veCPE 1U Unit (a host system with two power modules).

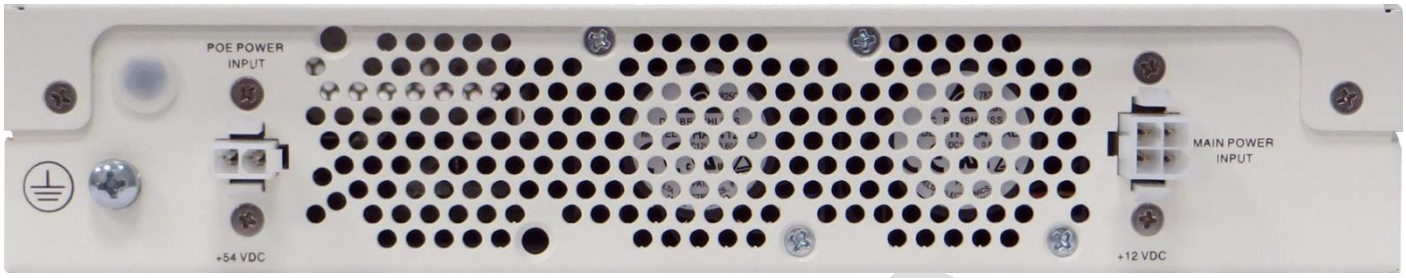


Figure 5. vE-CPE 1U Unit rear panel 54 VDC POE Power and 12 VDC Main Power

6. Installation

This chapter provides instructions on how to install the uBMC.

To install the uBMC, do the following:

Step 1: Mount the uBMC into the rack. The uBMC is ready for rack-mounting box.

Step 2: Connect AC/DC power converter to the 110/230 AC power supply.

For the 12 VDC uBMC Unit, connect power cable to the AC/DC power converter and
connect power connector to the 12VDC Main Power Input on the rear panel.
The Top and Bottom LEDs on the front panel turns on.

For the +54VDC uBMC Unit, connect power cable to the AC/DC power converter and
connect power connector to the 54VDC POE Power Input on the rear panel.
The Top and Bottom LEDs on the front panel turns on.

Step 3: Connect the RS232 DB9 management cable by doing the following:

1. Connect one end of the RS232 DB9 cable to the uBMC Management RS232 port.
2. Connect the other end of the RS232 cable to UART.
3. Use any terminal emulation software (Minicom, HyperTerminal, etc.) to connect to the CLI.
4. Set the following terminal communication parameters:
   - 115200 – default or 9600 if set by CLI command
   - 8 bits
   - no parity
   - 1 stop bit

- no flow control

5. Turn on the uBMC.

6. When the login prompt is displayed, log in with the following default parameters:
   - User name: **is_admin**
   - Password: **1qaz2wsX**
7. After login, change your password, user name and date. If you plan to use the management Ethernet port, set the IP address, net mask and gateway parameters.

Step 4: Connect the Ethernet management port.

1. Connect Ethernet cable (CAT5) to the Management 1G Ethernet network port.
2. Use any SSH or serial console to connect to the CLI.
3. The following are the default IP and login parameters:
   - IP address: 192.168.1.254
   - Net mask: 255.255.255.0
   - Gateway: 192.168.1.1
   - Login name: **is_admin**
   - Password: **1qaz2wsX**

7. Command line interface (CLI)

This chapter explains command names and command functions.
To view the full command list and to quickly navigate to the descriptions of each command, use the Table of Contents of this user guide.

7.1 CLI Features

The CLI supports auto complete with **TAB** key and it also supports displaying online help with "**?**".
Each command parameter can include any letter or number and '_', '/', '.', ';', '.','-' characters. But cannot contain any spaces.

7.2 Login

To log in to the command line interface (CLI), use serial console software and a serial cable to connect to the RS232 management port or use SSH to connect to the management IP of the uBMC device.
Once connected, the login prompt will be shown

```
<System Banner>
uBMC Login:
```

Use the following username and password as the default to access the CLI
Username: **is_admin**
Default Password:**1qaz2wsX**

Once logged in, the system prompt will be shown

```
uBMC>
```

7.3 Command modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands.

The following sections describe the following command modes:

- Command mode: user_exec
- Command mode: privileged_exec
- Command mode: configure

After login, the default mode would be user_exec, to go into privileged_exec use the "enable" command.
To go into the configure mode, use the "configure' command.

Notes:

- EXEC commands are not saved when the software reboots.

- Commands issued in a configuration mode can be saved to the startup configuration. When the running configuration is saved to the startup configuration, these commands will execute when the software is rebooted.

7.4 Command descriptions

This section provides descriptions to all commands.

<data-type> means the value need to input.

<choice> means the value should be chosen from a runtime list which can be shown with **TAB** key.

{a|b|c} means static multiple choices.

[…] means optional parameters.

7.4.1 Command Mode: user_exec

7.4.1.1 cli clear-history

Clear the CLI history for the current user.

7.4.1.2 enable

Enter enable mode.

7.4.1.3 exit

Log out of the CLI.

7.4.1.4 help

View the interactive help system.

7.4.1.5 show cli

Display CLI options.

7.4.1.6 show clock

Display system time and date.

7.4.1.7 show com configured

Display serial console configuration.

7.4.1.8 show device

Display device information.

7.4.1.9 show health

Display device health status.

7.4.1.10 show management configured

Display system management configuration.

7.4.1.11 show name configured

Display device name configuration.

7.4.1.12 show session configured

Display session configuration.

7.4.1.13 show users

Display a list of user accounts.

7.4.1.14 show version

Display version information for current system image.

7.4.2 Command Mode: privileged_exec

7.4.2.1 cli clear-history

Clear the CLI history for the current user.

7.4.2.2 configure

Enter configuration mode.

7.4.2.3 clock set date <*YYYY-MM-DD*>

Set the system date.

7.4.2.4 clock set time <*hh:mm:ss*>

Set the system time.

7.4.2.5 disable

Exit enable mode.

7.4.2.6 exit

Log out of the CLI.

7.4.2.7 help

View the interactive help system.

7.4.2.8 show cli

Display CLI options.

7.4.2.9 show clock

Display system time and date.

7.4.2.10 show com configured

Display serial console configuration.

7.4.2.11 show cpu

Display CPU usage.

7.4.2.12 show device

Display device information.

7.4.2.13 show health

Display device health status.

7.4.2.14 show log configured

Display log configuration.

7.4.2.15 show log [filter *<string>*]

Display log, and if filter keyword specified, only lines with keyword will be displayed.

Log viewer commands:
↑↓: move up/down a line.
ENTER: move down a line.
SPACE: scroll down one window.
g: go to the beginning of the log.
G: go to the end of the log.
/<keyword>: search down for the first line with keyword.
?<keyword>: search up for the first line with keyword.
q|Q: quit the log viewer and return to command line.

7.4.2.16 show log realtime

Display realtime log, use **CTRL+C** to quit the realtime viewer.

7.4.2.17 show management configured

Display system management configuration.

7.4.2.18 show memory

Display system memory usage.

7.4.2.19 show name configured

Display device name configuration.

7.4.2.20 show ntp configured

Display NTP configuration.

7.4.2.21 show radius configured

Display RADIUS configuration.

7.4.2.22 show session

Display session runtime state.

7.4.2.23 show session configured

Display session configuration.

7.4.2.24 show snmp {configured|engineID}

Display SNMP configuration or engine ID of the local system.

7.4.2.25 show ssh configured

Display SSH configuration.

7.4.2.26 show storage

Display storage usage.

7.4.2.27 show tacacs configured

Display TACACS+ configuration.

7.4.2.28 show users

Display a list of user accounts.

7.4.2.29 show version

Display version information for current system image.

7.4.2.30 show web configured

Display Web configuration.

7.4.2.31 reload [{force|noconfirm}]

Reboot the system.

Parameters:
force: Force an immediate reboot of the system even if it is busy.
noconfirm: Reboot the system without asking whether to save changes.

7.4.2.32 write memory

Save running configuration to the active configuration file.

7.4.3 Command Mode: configure

bmc console connect

Connect to host console

3.2 **bmc console connect force**

Force connecting even if someone is already connected

3.3 **bmc console log to-file**

Enable writing log to file

3.4 **bmc console log rotate-num** *<1-50>*

Configure the log rotate number

3.5 **bmc console log rotate-size** *<1-10(MB)>*

Configure the log rotate size

3.6 **bmc console speed** <*9600*|*38400*|*115200*>

Configure host console baudrate

Parameters:

9600:

38400:

115200:

3.7 **bmc console data** <*5*|*6*|*7*|*8*>

Configure host console data bits

Parameters:

5:

6:

7:

8:

3.8 **bmc console parity** <*none*|*even*|*odd*|*mark*|*space*>

Configure host console parity

Parameters:

none:

even:

odd:

mark:

space:

3.9 **bmc console stopbits** <*1*|*2*>
Configure host console stopbits
Parameters:
1:
2:

3.10 **bmc console hw-flowctrl**
Enable hardware flow control

3.11 **bmc console sw-flowctrl**
Enable software flow control

3.12 **bmc power** <*on*|*off*|*forceoff*|*cycle*|*reset*>
Configure BMC host power
Parameters:
on: Power on host
off: Power off host
forceoff: Force power off host
cycle: Power cycle host
reset: Power reset host

3.13 **bmc bios upgrade file-url** <*url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file*> [*all*]
Upload a BIOS image from an HTTP/HTTPS/SCP/FTP URL
Parameters:
all: Upgrade all flash regions

3.14 **bmc usb-cdrom upload** <*url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file*>
Upload an ISO file with default name is_cdrom_yyyymmddHHMMSS

3.15 **bmc usb-cdrom upload** <*url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file*> **as** <*select from list*>
Save an uploaded ISO file as the given name

3.16 **bmc usb-cdrom attach-local image** <*select from list*>
Attach a local ISO image as CDROM to the host USB
Parameters:
image: The local image file

3.17 **bmc usb-cdrom attach-remote host** <*hostname*> **path** <*path as /path/file*> **user** <*username*> [*password* <*password*>]

Attach a remote ISO image as CDROM to the host USB

Parameters:

host: The remote host address

path: The full shared path for the image file

user: The login user name

password: The login user password

3.18 **bmc usb-cdrom detach**

Detach a previously attached ISO image

3.19 **bmc sel clear**

Clear all SEL log entries

7.4.3.1 cli clear-history

Clear the CLI history for the current user.

7.4.3.2 clock set date *<YYYY-MM-DD>*

Set the system date.

7.4.3.3 clock set time *<hh:mm:ss>*

Set the system time.

7.4.3.4 clock timezone *<choice>* area *<choice>*

Set the system time zone.

Parameters:

timezone: the system time zone.

area: the area in the time zone.

7.4.3.5 com speed {9600|38400|115200}

Configure serial console speed.

Parameters:

9600: set speed to 9600.
38400: set speed to 38400.
115200: set speed to 115200.

7.4.3.6 com terminal-type *<string>*

Configure serial console terminal type such as vt100/vt102/ANSI.

7.4.3.7 configurations save [as *<string>*]

Save current configuration to a file (if filename not specified, default is_config_yyyymmddHHMMSS).

Parameters:
as: filename

7.4.3.8 configurations upload <url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file> [as <string>]

Upload a configuration file (if filename not specified, default is_config_yyyymmddHHMMSS).

Parameters:
url: SCP URL such as xxx@x.x.x.x:/path/file.
as: filename.

7.4.3.9 configurations restore *<choice>*

Restore system configuration from the previously saved of uploaded configuration file and.

7.4.3.10 configurations reset

Reset system to the default configuration and reboot.

7.4.3.11 dump create log

Create a system log dump file as is_log_YYYYMMDDhhmmss.

7.4.3.12 dump delete *<choice>*

Delete a system dump file.

7.4.3.13 exit

Exit configuration mode.

7.4.3.14 help

View the interactive help system.

7.4.3.15 log level {debug|info|notice|warn|err|crit|alert|emerg}

Configure the system log level.

Parameters:
debug: DEBUG.
info: INFO.
notice: NOTICE.
warn: WARNING.
err: ERROR.
crit: CRITICAL.
alert: ALERT.
emerg: ERMRGENCY.

7.4.3.16 log max-size *<integer>*

Configure the maximum log file size, 1-10 MB.

7.4.3.17 log reset

Reset all system logs.

7.4.3.18 log remote {disable|enable}

Enable or disable remote log.

7.4.3.19 log remote server *<hostname or IP>* [port *<port number>*]

Add a remote log server, and default port is 514.

7.4.3.20 login-banner <The new banner string, using '\' as escape>

Configure device login banner

7.4.3.21 management interface <interface name> device <device name> vlan <2-4094>

Add a VLAN interface on the net device

Parameters:

interface: Configure ethernet interface

vlan: Configure interface VLAN ID

7.4.3.22 management interface <select from list> enable

Enable ethernet interface

Parameters:

interface: Configure ethernet interface

7.4.3.23 management interface <select from list> desc <string>

Configure interface description

Parameters:

interface: Configure ethernet interface

7.4.3.24 management interface <select from list> master <select from list>

Configure interface master device

Parameters:

interface: Configure ethernet interface

7.4.3.25 management interface <select from list> mtu <MTU size > 68>

Configure interface MTU size

Parameters:

interface: Configure ethernet interface

7.4.3.26 management interface <select from list> dhcp-sendname

Configure sending hostname when DHCP

Parameters:

interface: Configure ethernet interface

7.4.3.27 management interface <select from list> ipv4 enable

Enable IPV4

Parameters:

interface: Configure ethernet interface

7.4.3.28 management interface <select from list> ipv4 static [ip <IPV4 address>] [prefixlen <0-32>]

Enable IPV4 static address
Parameters:
interface: Configure ethernet interface
ip: Configure IPV4 IP
prefixlen: Configure IPV4 prefix length

7.4.3.29 management interface <select from list> ipv4 ip <IPV4 address>

Configure IPV4 IP
Parameters:
interface: Configure ethernet interface

7.4.3.30 management interface <select from list> ipv4 prefixlen <0-32>

Configure IPV4 prefix length
Parameters:
interface: Configure ethernet interface

7.4.3.31 management interface <select from list> ipv4 dhcp

Enable IPV4 DHCP
Parameters:
interface: Configure ethernet interface

7.4.3.32 management interface <select from list> ipv6 static [ip <IPV6 address>] [prefixlen <0-128>]

Enable IPV6 static address
Parameters:
interface: Configure ethernet interface
ip: Configure IPV6 IP
prefixlen: Configure IPV6 prefix length

7.4.3.33 management interface <select from list> ipv6 ip <IPV6 address>

Configure IPV6 IP

Parameters:
interface: Configure ethernet interface

7.4.3.34 management interface <select from list> ipv6 prefixlen <0-128>

Configure IPV6 prefix length
Parameters:
interface: Configure ethernet interface

7.4.3.35 management interface <select from list> ipv6 dhcp

Enable IPV6 DHCP
Parameters:
interface: Configure ethernet interface

7.4.3.36 management secondary-address <address name> ip <IPV4/IPV6 address> prefixlen <0-128> interface <select from list>

Add a secondary address
Parameters:
ip: IP address
prefixlen: IP address prefix length
interface: Interface name

7.4.3.37 management vrf <VRF name> table <number>

Add a VRF routing table
Parameters:
table: VRF table ID

7.4.3.38 management vrf-process <VRF process binding name> process <select from list> vrf <select from list> binding-address <IP list seperated by ','>

Add a VRF process
Parameters:
process: process name
vrf: VRF name
binding-address: Binding IP address

7.4.3.39 management route <route name> dest <ip subnet like 192.168.0.0/24> via <ip address> dev <select from list> metric <number> table <number>

Add an IP route, using '' for unused option

Parameters:

dest: Destination address

via: Next hop address

dev: Routing device

metric: Routing metric

table: Route table ID

7.4.3.40 management default-gw <IP address>

Configure default gateway

7.4.3.41 management dns server <IP address>

Add a DNS server

7.4.3.42 management ipsec enable

Enable IPsec

7.4.3.43 management ipsec connection <connection name>

Add/Modify an IPsec connection

7.4.3.44 management ipsec connection <select from list> tries <a positive integer or %forever>

Attempts to negotiate

7.4.3.45 management ipsec connection <select from list> ike <encryption-integrity[-prf]-dhgroup>

IKE SA enc/auth algorithms

7.4.3.46 management ipsec connection <select from list> esp <encryption-integrity[-dhgroup][-esnmode]>

ESP enc/auth algorithms

7.4.3.47 management ipsec connection <select from list> compress <yes|no>

IPComp compression of content
Parameters:
yes: Turn on compression
no: Turn off compression

7.4.3.48 management ipsec connection <select from list> replay-window <-1|0|[size]>

Replay window size

7.4.3.49 management ipsec connection <select from list> dpdaction <none|clear|hold|restart>

Controls the use of the Dead Peer Detection protocol
Parameters:
none: Disables the active sending of DPD messages
clear: The connection is closed
hold: Re-negotiate the connection on demand
restart: Re-negotiate the connection

7.4.3.50 management ipsec connection <select from list> dpddelay <0|[number]s>

The interval to send DPD messages

7.4.3.51 management ipsec connection <select from list> dpdtimeout <[number]s>

The timeout interval to delete all connections to a peer in case of inactivity

7.4.3.52 management ipsec connection <select from list> ikelifetime <[number][s|m|h|d]>

How long the keying channel of a connection should last

7.4.3.53 management ipsec connection <select from list> lifetime <[number][s|m|h|d]>

How long a particular instance of a connection should last

7.4.3.54 management ipsec connection <select from list> local-ip <IP/hostname/%any/%any6>

Local IP

7.4.3.55 management ipsec connection <select from list> local-id <Authentication ID>

Local authentication ID

7.4.3.56 management ipsec connection <select from list> local-id2 <Authentication ID>

Local additional authentication ID

7.4.3.57 management ipsec connection <select from list> local-src <IP/%any/%config>

Local virtual IP

7.4.3.58 management ipsec connection <select from list> local-sub <IP subnet>

Local private subnet

7.4.3.59 management ipsec connection <select from list> local-auth <select from list>

Local authentication methord

7.4.3.60 management ipsec connection <select from list> local-auth2 <select from list>

Local additional authentication methord

7.4.3.61 management ipsec connection <select from list> local-cert <select from list>

Local certificate

7.4.3.62 management ipsec connection <select from list> local-cert2 <select from list>

Local certificate

7.4.3.63 management ipsec connection <select from list> peer-ip <IP/hostname/%any/%any6>

Peer IP

7.4.3.64 management ipsec connection <select from list> peer-id <Authentication ID>

Peer authentication ID

7.4.3.65 management ipsec connection <select from list> peer-id2 <Authentication ID>

Peer additional authentication ID

7.4.3.66 management ipsec connection <select from list> peer-src <IP/%any/%config>

Peer virtual IP

7.4.3.67 management ipsec connection <select from list> peer-sub <IP subnet>

Peer private subnet

7.4.3.68 management ipsec connection <select from list> peer-auth <select from list>

Peer authentication methord

7.4.3.69 management ipsec connection <select from list> peer-auth2 <select from list>

Peer additional authentication methord

7.4.3.70 management ipsec connection <select from list> peer-cert <select from list>

Peer certificate

7.4.3.71 management ipsec connection <select from list> peer-cert2 <select from list>

Peer certificate

7.4.3.72 management ipsec ca <ca name> cacert <select from list> ocspuri <URI>

Add an IPsec Certification Authority

Parameters:

cacert: The certificate

ocspuri: OCSP URI

7.4.3.73 management ipsec secret <secret name> psk key [host <IP/FQDN/user@FQDN/%any/%any6>] [peer <IP/FQDN/user@FQDN/%any/%any6>]

Add a PSK secret

Parameters:

secret: Add an IPsec secret

key: Pre-share key

host: Host ID
peer: Peer ID

7.4.3.74 management ipsec secret <secret name> eap user <user ID> secret <secret>

Add an EAP credentials
Parameters:
secret: Add an IPsec secret
user: EAP user ID
secret: EAP secret

7.4.3.75 management ipsec secret <secret name> xauth user <user ID> pass <password>

Add an XAUTH credentials
Parameters:
secret: Add an IPsec secret
user: XAUTH user ID
pass: XAUTH password

7.4.3.76 management ipsec secret <secret name> rsa key <select from list> [pass <passphrase>]

Add an RSA key
Parameters:
secret: Add an IPsec secret
key: RSA private key
pass: passphrase if the private key file is encrypted

7.4.3.77 management ipsec secret <secret name> ecdsa key <select from list> [pass <passphrase>]

Add an ECDSA key
Parameters:
secret: Add an IPsec secret
key: ECDSA private key
pass: passphrase if the private key file is encrypted

7.4.3.78 management ipsec key <key identifier> file-url <url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file>

Upload a key file from an HTTP/HTTPS/SCP URL

Parameters:
key: Add a private key

7.4.3.79 management ipsec key <key identifier> raw <key content>

Add a key with raw content, using '\' as escape
Parameters:
key: Add a private key

7.4.3.80 management ipsec cert <certificate identifier> file-url <url such as http://xxx/file or scp://xxx@x.x.x.x:/path/file>

Upload a certificate file from an HTTP/HTTPS/SCP URL
Parameters:
cert: Add a certificate

7.4.3.81 management ipsec cert <certificate identifier> raw <cert content>

Add a certificate with raw content, using '\' as escape
Parameters:
cert: Add a certificate

7.4.3.82 management permitted {disable|enable}

Enable or disable management permitted IP filter.

7.4.3.83 management permitted ip *<IP>* [mask *<IP net mask>*]

Add a permitted IP address, and default mask is 255.255.255.255.

7.4.3.84 management whoami {off|on}

Turn on/off the whoami function, which is designed for rack identification. When the function is turned on, the Sys OK LED blinks every second.

7.4.3.85 name *<hostname>*

Configure device name, which will be shown in CLI prompt, and the valid format should be [a-zA-Z0-9-_.]

7.4.3.86 no configuration *<choice>*

Remove a system configuration file.

7.4.3.87 no log-server *<choice>*

Remove a log remote server.

7.4.3.88 no management dns *<choice>*

Remove a management DNS server.

7.4.3.89 no management permitted *<choice>*

Remove a management permitted IP

7.4.3.90 no ntp-server *<choice>*

Remove an NTP server.

7.4.3.91 no radius *<choice>*

Remove a RADIUS server.

7.4.3.92 no snmp community *<choice>*

Remove an SNMP community.

7.4.3.93 no snmp host *<choice>*

Remove an SNMP trap host.

7.4.3.94 no snmp user *<choice>*

Remove an SNMP trap user.

7.4.3.95 no tacacs *<choice>*

Remove a TACACS+ server.

7.4.3.96 no user *<choice>*

Remove a local user account.

7.4.3.97 ntp {disable|enable}

Enable or disable NTP.

7.4.3.98 ntp server *<hostname or IP>*

Add an NTP server.

Note: if the NTP server is a host like pool.ntp.org, the dns server must be configured to make it work.

7.4.3.99 radius {disable|enable}

Enable or disable RADIUS login.

7.4.3.100 radius local-login {disable|enable}

Enable or disable local users' login when RADIUS enabled. For details, refer to 3. System management overview.

7.4.3.101 radius privilege {readonly|normal|admin}

Configure RADIUS user privilege.

Parameters:
readonly: read-only access.
normal: normal read and write access.
admin: administrator's access.

7.4.3.102 radius retry *<integer>*

Configure RADIUS login max retry count.

7.4.3.103 radius server *<ID number>* ip *<IP>* port *<port number>* secret *<string>* timeout *<integer>*

Add a RADIUS server

Parameters:
ip: RADIUS server IP.

port: RADIUS server port.
secret: server secret, 8-128 symbols.
timeout: connect timeout in seconds.

7.4.3.104 reload [{switch-software|force|noconfirm}]

Reboot the system.

Parameters:
switch-software: reboot the system and switch current firmware to backup software.
force: force an immediate reboot of the system even if it is busy.
noconfirm: reboot the system without asking whether to save changes.

7.4.3.105 reset

Reset the system to factory setting and reboot.

7.4.3.106 session expired-time *<integer>*

Specify the time in seconds after which an idle session is expired, 0 means disabling expiration check.

7.4.3.107 show cli

Display CLI options.

7.4.3.108 show clock

Display system time and date.

7.4.3.109 show com configured

Display serial console configuration.

7.4.3.110 show configurations list

Display system configuration file list.

7.4.3.111 show configurations detail *<choice>*

Display system configuration file in detail.

7.4.3.112 show cpu

Display CPU usage.

7.4.3.113 show device

Display device information.

7.4.3.114 show dump

Display system dump file list.

7.4.3.115 show health

Display device health status, including sensor temperature and fan status.

7.4.3.116 show log configured

Display log configuration.

7.4.3.117 show log [filter *<string>*]

Display log, and if filter keyword specified, only lines with keyword will be displayed.

Log viewer commands:
↑↓: move up/down a line.
ENTER: move down a line.
SPACE: scroll down one window.
g: go to the beginning of the log.
G: go to the end of the log.
/<keyword>: search down for the first line with keyword.
?<keyword>: search up for the first line with keyword.
q|Q: quit the log viewer and return to command line.

7.4.3.118 show log realtime

Display realtime log, use **CTRL+C** to quit the realtime viewer.

7.4.3.119 show management configured

Display system management configuration.

7.4.3.120 show memory

Display system memory usage.

7.4.3.121 show ntp configured

Display NTP configuration.

7.4.3.122 show radius configured

Display RADIUS configuration.

7.4.3.123 show session

Display session runtime state.

7.4.3.124 show session configured

Display session configuration.

7.4.3.125 show snmp {configured|engineID}

Display SNMP configuration or engine ID of the local system.

7.4.3.126 show ssh configured

Display SSH configuration.

7.4.3.127 show storage

Display storage usage.

7.4.3.128 show tacacs configured

Display TACACS+ configuration.

7.4.3.129 show uptime.

Display system uptime information.

7.4.3.130 show users

Display system local user list.

7.4.3.131 show version

Display version information for current system image.

7.4.3.132 show web configured

Display web configuration.

7.4.3.133 snmp {disable|enable}

Enable or disable SNMP server service.

7.4.3.134 snmp apply

Apply SNMP configuration. The user needs to run this command for any of the following configuration to take effect:
snmp community <*choice*> [*disable*|*enable*|*full-access*|*read-only*]
snmp host <*choice*> <*disable*|*enable*>
snmp user <*choice*> <*disable*|*enable*|*full-access*|*read-only*>

7.4.3.135 snmp community *<string>*

Add an SNMP v1/v2c community.

7.4.3.136 snmp community *<choice>* {disable|enable|full-access|read-only}

Configure an SNMP v1/v2c community.
Note: The user need to run the **snmp apply** command for this configuration to take effect.

Parameters:
disable: disable the user.
enable: enable the user.
full-access: grant full access.
read-only: grant read-only access.

7.4.3.137 snmp host *<choice>* {disable|enable}

Enable or disable a host to send SNMP traps to.

Note: The user need to run the **snmp apply** command for this configuration to take effect.

7.4.3.138 snmp host *<hostname or IP>* {v1|v2c} community *<string>*

Add an SNMP v1/v2c trap host.

Parameters:

v1: SNMP Version 1.

v2c: SNMP Version 2C.

community: community name.

7.4.3.139 snmp host *<hostname or IP>* v3 user *<string>* password *<string>* {md5|sha}

Add an SNMP Version 3 trap host.

Parameters:

user: login user, 5-30 symbols.

password: login password in plain text, at least 8 symbols.

md5: use the MD5 hash algorithm.

sha: use the SHA1 hash algorithm.

7.4.3.140 snmp threshold fan {min|max} *<integer>*

Configure minimal or max threshold of fan speed.

Parameters:

min: minimal threshold, 100-10000 RPM.

max: max threshold, 10000-40000 RPM.

7.4.3.141 snmp threshold sensor {bcm-max|switch-max|module-max|port-max} *<integer>*

Configure sensor temperature threshold.

Parameters:

bcm-max: BCM max temperature threshold, 60-90 °C.

switch-max: switch max temperature threshold, 60-90 °C.

module-max: module max temperature threshold, 60-90 °C.
port-max: port max temperature threshold, 60-90 °C.

7.4.3.142 snmp trap {disable|enable} {all|application|fan|power|sensor|switch|system|threshold|terminal}

Enable or disable an SNMP trap type.

Parameters:
all: all trap types.
application: application trap.
fan: fan trap.
power: power trap.
sensor: sensor trap.
switch: switch trap.
system: system trap.
threshold: threshold trap.
terminal: terminal trap.

7.4.3.143 snmp user *<choice>* {disable|enable|full-access|read-only}

Configure an SNMP v3 access user account.
Note: The user need to run the **snmp apply** command for the configuration to take effect.

Parameters:
disable: Disable the user's access.
enable: Enable the user's access.
full-access: grant full access.
read-only: grant read-only access.

7.4.3.144 snmp user *<string>* password *<string>* {md5|sha}

Add an SNMP v3 user.

Parameters:
user: username, 5-30 symbols.
password: password in plain text, at least 8 symbols.
md5: use the MD5 hash algorithm
sha: use the SHA1 hash algorithm

7.4.3.145 ssh {disable|enable}

Enable or disable SSH service.

7.4.3.146 ssh port *<port number>*

Configure SSH service port, default 22.

7.4.3.147 tacacs {disable|enable}

Enable or disable TACACS+ remote login. For details, refer to 3. System management overview.

7.4.3.148 tacacs local-login {disable|enable}

Enable or disable local users' login when TACACS+ enabled. For details, refer to 3. System management overview.

7.4.3.149 tacacs service *<string>*

Configure TACACS+ service tag. For details, refer to 3. System management overview.

7.4.3.150 tacacs timeout *<integer>*

Configure TACACS+ connect timeout in seconds.

7.4.3.151 tacacs server *<ID number>* ip *<IP>* port *<port number>* secret *<string>*

Add a TACACS+ server.

Parameters:
secret: server secret, 8-128 symbols.

7.4.3.152 test bypass {all|module|segment} *<choice>*

Run the auto test for the bypass.

Parameters:
all: test all segments of the bypass.
module: test all segments of the specific module.
segment: test the specific segment.

7.4.3.153 upgrade ftp *<url>* user *<string>* password *<string>*

Upgrade system from an FTP URL.

Parameters:
url: FTP URL such as ftp://x.x.x.x/path/file.
user: FTP user name.
password: FTP user password.

7.4.3.154 upgrade http *<url>*

Upgrade system from an HTTP URL such as http://x.x.x.x/path/file.

7.4.3.155 upgrade scp *<url>* user *<string>*

Upgrade system from an SCP URL.

Parameters:
scp: an SCP URL such as scp://x.x.x.x/path/file.
user: SSH user name.

7.4.3.156 user change-password {new-password|new-encrypt-password} *<string>* [user-name *<choice>*]

Change the local user's password.

Parameters:
new-password: password in plain text, 6-40 symbols.
new-encrypt-password: password in encrypted text, 8-128 symbols.
user-name: specify the local user, else the current user password will be changed.

7.4.3.157 user name *<string>* full-name *<string>* {password|encrypt-password} *<string>* privilege {readonly|normal|admin}

Add a local user account.

Parameters:
name: 1-31 symbols.
full-name: a description such as 'Adam Bush'.
new-password: password in plain text, 6-40 symbols.
new-encrypt-password: password in encrypted text, 8-128 symbols.

privilege: user privilege.
readonly: read-only access
normal: normal read and write access
admin: administrator's access

7.4.3.158 web session-expired-time *<integer>*

Specify the time in seconds after which an idle Web session is expired, 60~3600 seconds.

7.4.3.159 web http {disable|enable}

Enable or disable HTTP service

7.4.3.160 web http port *<port number>*

Configure HTTP listening port, default 80.

7.4.3.161 web https {disable|enable}

Enable or disable HTTPS service.

7.4.3.162 web https port *<port number>*

Configure HTTPS listening port, default 443.

7.4.3.163 web https ssl {cert|key} file-url *<url>*

Configure the HTTPS SSL certificate or key file from a SCP URL like xxx@x.x.x.x:/path/file.

7.4.3.164 web https ssl {cert|key} encrypt *<string>*

Configure the HTTPS SSL certificate or key with an encrypted string.

7.4.3.165 write memory

Save running configuration to the active configuration file.

8. Web Interface

This chapter introduces the uBMC Web interface.

8.1 Starting the Web interface

The uBMC Web interface can be accessed from most popular Web browsers. To connect to the uBMC Web interface, use the following Web addresses on your Web browser:

- If http is enabled, use “http://device_ip_address”; if the http port is not the default **80**, use http://device_ip_address:http_port
- If https is disabled, use “https://device_ip_address”; if the https port is not the default **443**, use https://device_ip_address:https_port

where **device_ip_address** is the uBMC Ethernet management port IP address.

Notes:

- If the Web interface has been inactive (not sending requests to the uBMC) for a period longer than the specified Web Session Timeout value (default: 900 seconds), a login screen will be displayed. The user can configure the Web Session Timeout value by navigating to **System > Service > Web > Session Timeout**.
- Context help is provided for most Web application fields.
- All the new settings in the Web interface take affect only after the user clicks the **Commit** button.

8.2 Login

The following screenshot shows the login screen of the uBMC Web interface.

On the login screen, type the user name and password to access the uBMC Web interface. The default user name is **is_admin**. The default password is **1qaz2wsX**.

The first user that logs into the Web interface will get full rights (control and monitor) in the Web interface. The following users will not be able to control the Web interface, and they will only be able to monitor the uBMC parameters.

When the first user logs off from the Web interface, the next user will inherit the first user's rights and will be able to control and monitor the Web interface.

After login, the main menu of the uBMC Web interface is displayed, which contains the following tabs:

Each tab will be explained in subsequent sections.

8.3 Status

The **Status** tab provides access to the following status information pages:

- **System**
- **SNMP**
- **Session**
- **System Log**

8.3.1 System

Navigate to **Status > System>System Information** to view the following system status:

- **Global**
- **System Events**
- **System Interfaces**
- **System DHCP**
- **System Iptables**
- **System IPsec**
- **Host Fan Status**
- **Host Voltage Status**
- **Host Temperature Status**
- **Power Supply Status**

The **Global** area provides the following information:

- **Device Type**: Device Name
- **Device Serial Number**: Device Serial Number
- **Hardware Version**: Device Hardware version
- **Software Version**: Device Software version
- **UBoot Version**: Device UBoot version
- **System Time:** The current system time
- **System Uptime:** How long the system has been running
- **Load average:** The average system load over a period of time.
  It conventionally appears in the form of three numbers,
  which represent the system load during the last one-, five-, and fifteen-minute periods.
- **Config Change Saved:** Whether the configuration is saved to non-volatile memory.

The **System Events** area shows the critical events in the system
(These section contains no values yet)

The **System Interfaces** area shows the following interfaces:

- **eth0**: management interface Eth0 networking info
- **eth1**: management interface Eth1 networking info

The **System DHCP** area shows the following information:

- **State**: DHCP state status (running or not running)
- **Leases**: DHCP lease interface name, ip address, dhcp options parameters

The **System Iptables** area shows the iptables information:

Input Accept, Forward Accept, Output Accept, Iptables configured options

The **System IPSEC** area provides the following information:

- **IPSEC**: IPSEC connection status and IPSEC parameters info

The **Host Fan Status** area provides the following information:

- **FAN1**: Fault, Warning, Status and Speed (RPM)
- **FAN2**: Fault, Warning, Status and Speed (RPM)
- **FAN3**: Fault, Warning, Status and Speed (RPM)

The **Host Voltage Status** area provides the following information:

- **5V**: 5V Voltage nominal value in the unit
- **3.3V**: 3.3V Voltage nominal value in the unit
- **CPU_VCCSRAM**: CPU Voltage nominal value in the unit
- **CPU_VCCP**: CPU Voltage nominal value in the unit
- **1.05V**: 1.05V Voltage nominal value in the unit
- **MEM_VDDQ**: 3.3V Voltage nominal value in the unit
- **CPU_VNN**: 1.05V Voltage nominal value in the unit
- **1.8V**: 1.8V Voltage nominal value in the unit

The **Host Temperature Status** area provides the following information:

- **TEMP_HOST_CPU**: average and peak temperature on the host
- **TEMP_HOST_PCB**: average and peak temperature of the pcb
- **TEMP_INLET_AMB**: ambient and peak temperature inside the unit

The **Power Supply Status** area shows the power supply information:
(These section contains no values yet)

8.3.2 SNMP

Navigate to **Status > System** to view the following system status:
(These section contains no values yet)

8.3.3 Session

Navigate to **Status > Session** to view the following information:

- **ID**: User ID number
- **User**: User name
- **Login Type**: Web or Cli

- **Login Time**: User login time
- **Login IP**: User login ip
- **Login Port**: User login port

8.3.4 System Log

Navigate to **Status > System Log** to view the System log info:
Scroll between the pages to retrieve the **System Log** information:

Tips for reviewing the system log:

- The log is displayed in backward scheduling order. The latest events are displayed on the first page while the earliest events on the last page.
- Select or type a page number to review the log on a selected page.
- Input key words and click **Search** to filter the log.
- To clear all the logs, click **Reset Log**.

8.4 System

The **System** tab provides access to the following system information pages:

- **General**
- **Service**
- **Management Interface**
- **IPsec**
- **Iptables**
- **Keys/Certs**
- **Configurations**
- **System Dump**
- **Upgrade/Switch**
- **Reboot/Reset**

8.4.1 General

Navigate to **System > General Configuration** to view or modify general system settings.

- **System:** Device Name and CLI Login Banner
- **DateTime:** Timezone; New Date; New Time and NTP Enabled
- **NTP Server:** Host or IPV4 address
- **Log:** Log Level; Max Log File Size; Remote Log enabled
- **Log Server:** Host; Port

In the **System** area, the user can configure the device name (default name is **ubmc**).
In the **DateTime** area, the user can configure the following:

- **Timezone:** The default time zone is UTC.
- **New Date:** Set the system date.
- **New Time:** Set the system time.
- **NTP Enabled:** To synchronize system clock using the NTP protocol.
- **NTP Server:** Add/remove the NTP server using the server IP or hostname. If the NTP server is an internet host like pool.ntp.org, the dns server must be configured to make it work.

In the **Log** area, the user can configure the following:

- **Log Level: DEBUG**, **INFO**, **NOTICE**, **WARNING**, **ERROR**, **CRITICAL**, **ALERT**, **EMERGENCY**.
- **Max Log File Size:** the maximum log file size.
- **Remote Log Enabled:** To enable the remote log function. When enabled, the uBMC will send log messages to the specified remote log server. This function is disabled by default.
- **Remote Log Server IP:** Add/remove the remote server to receive the log messages.

8.4.2 Service Configuration

Navigate to **System > Service** to view or modify service settings.

The user can configure the following service settings:

- **COM:** Configure the serial COM settings, set the speed and terminal type.
- **SSH:** Configure the listening port. To regenerate SSH keys, click the **Re-generate SSH Keys** button.
- **Web**: Configure the Web **Session Timeout** value in seconds.
- **HTTP:** Enable or disable the http protocol and configure the listening port.
- **HTTPS:** Enable or disable the https protocol and configure the listening port.
  Upload files to update the SSL certificate and private key of the https service.

Note: Changing settings on this page may cause the current connection to be interrupted, and the user should reload the web page according to the new settings.

8.4.3 Management Interface

Navigate to **System > Management Interface** to view or configure management settings.

In the **Interfaces** area, the user can perform the following:

- Configure **Interface eth0** to activate in-band management network access.
  Interface Description pre-defined In-Band.
  The user can activate or dis-activate Current State.
  The user can configure the eth0 Interface MTU, VLAN
  The user can activate or dis-activate DHCP Send Hostname and IPv4/IPv6 Enable
  Select IPv4 and configure IPv4 Origin (Static/DHCP, management IPv4 address, mask and gateway.
  Select IPv6 and configure IPv6 Origin (Static/DHCP, management IPv4 address, mask and gateway.
- Configure **Interface eth1** to activate out-of-band management network access.
  Interface Description pre-defined Out-of-Band.
  The user can activate or dis-activate Current State.
  The user can configure the eth0 Interface MTU, VLAN
  The user can activate or dis-activate DHCP Send Hostname and IPv4/IPv6 Enable
  Select IPv4 and configure IPv4 Origin (Static/DHCP, management IPv4 address, mask and gateway.
  Select IPv6 and configure IPv6 Origin (Static/DHCP, management IPv4 address, mask and gateway.

In the **VRF List** area, the user can add/remove VRF.

In the **VRF Process List** area, the user can add/remove VRF processes.

In the **Route List** area shows VRF routing.

In the **Address List** area, the user can add/remove permitted addresses list.

In the **DNS server** area, the user can add/remove dns configuration parameters.

8.4.4 IPsec

Navigate to **System > IPsec** to configure IPsec State, IPsec Connections, Certificates (CA) and Secrets
In the **IPsec State** area, the user can perform the following:

- Enable or disable IPsec connection.

In the **IPsec Connections** area, the user can perform the following:

- Add IPsec connection name, Type (tunnel/transport/transport proxy/passthrough/drop),

Key Exchange (ike/ikev1/ikev2), IKE, ESP, Compress (yes/no), Replay-window, DPD Action (none/clear/hold/restart), DPD Delay, DPD Timeout, IKE Lifetime, Lifetime, Local IP, Local IDLocal source IP, Local Auth (pubkey/psk/eap/……..), Local Auth2 (pubkey/ Psk/eap/eap-aka/eap-gtc….), Local Cert, Local Cert2, Peer IP, Peer ID, Peer Source IP, Peer Subnet, Peer Auth, Peer Auth2, Peer Cert, Peer cert2

In the **IPsec CAs** area, the user can perform the following:

- Add IPsec CA name, CA Certificate, OCSP URI, CRL URI, Base URI

In the **IPsec Secrets** area, the user can perform the following:

- Add IPsec Secrets name, Type, Host/User, Peer, Key/ Password, key File, Passphrase

8.4.5 Iptables

Navigate to **System > Iptables** area to configure Iptables parameters.

8.4.6 Keys/Certs

Navigate to **System > Keys/Certs** area to configure Private Keys and Certificates

In the **Private Keys** area, the user can perform the following:

- Add **Key-ID** name, browse and download the private key

In the **Certificates** area, the user can perform the following:

- Add **Cert-ID** name, browse and download the certificate

8.4.7 Configurations

Navigate to **System > Configurations** to save and restore your configuration and reset the device to default settings.

The **Configuration List** area lists all available configuration files.
The user can select one configuration file and perform any of the following actions:

- **View:** view the chosen configuration file.
- **Restore:** restore the configuration defined in the chosen file.
- **Delete:** delete the chosen configuration file.
- **Download:** download the chosen configuration file.

In the **Save current configuration as** area, the user can save the current configurations.
In the **Upload a configuration file** area, the user can navigate to a configuration file and upload it.
In the **Reset to default configuration** area, the user can reset to the default configuration.

Note:
Although configurations downloaded is a text based file containing CLI commands, it can't be tampered with if the user wishes to upload it later back to the uBMC device.

8.4.8 System Dump

Navigate to **System > System Dump** to create, delete or download system dump files, including core-dump files and log files.

To create a system log dump file, click **Create**.
To delete a system dump file, select the file and click **Delete**.
To download a system dump file, click the file link.

8.4.9 Upgrade/Switch

Navigate to **System > Upgrade/Switch** to view the current software version or to upgrade/switch the firmware.

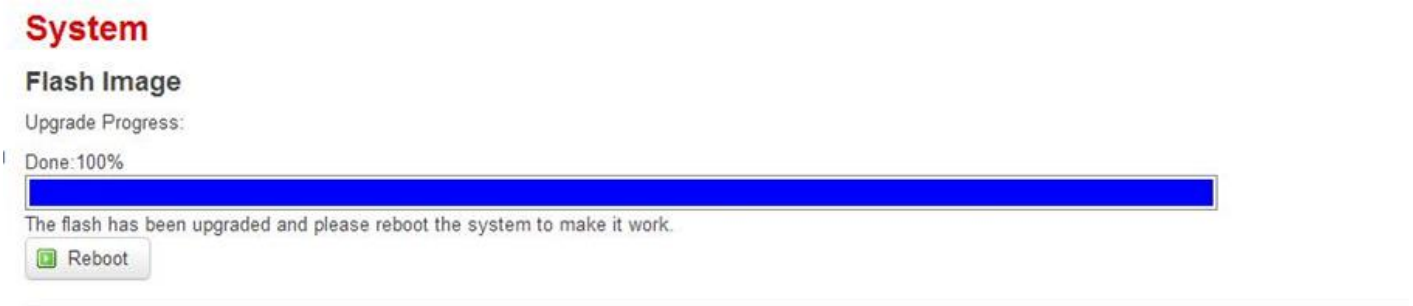
To switch the firmware between current version and backup version, just click “Switch”.

To upgrade the firmware, upload a newer version of firmware image by doing the following:

1. Click **Browse** to navigate to the intended firmware image file.
2. Click **Upload image**. If the image is correct, a confirmation window will be displayed, asking whether to proceed or not, as shown:

   Note: If the user closes the confirmation window without making a decision, the window will be displayed again when the user clicks **System > Upgrade.**

4. Click **Proceed**. A progress bar is displayed, as shown.



The upgrade process takes around 4 minutes, during which the user can stay on the progress page to watch the progress, or can go to other pages and return later to view the result.

4. When the upgrade process is finished, click **Reboot** to restart the system in order the new image to take effect.

8.4.10 Reboot/Halt/Reset

Navigate to **System > Reboot/Halt/Reset** to reboot or halt the system.

Click **Reboot** to restart the system. A reboot takes around one minute.

Click **Halt** to turn off the system.

Click **Reset** to reset the system to factory setting, which will reboot the system into the factory settings.

8.5 BMC

The **BMC** tab provides access to the following user configuration options:

- **Console Redirection**
- **Console Log**
- **Power Control**
- **BIOS**
- **USD CDROM**
- **System Event Log**

8.5.1 Console Redirection

Navigate to **BMC > Console Redirection** to view BMC Console Status or modify BMC Console Redirection.

BMC Console Status shows the Console Cable status connected or disconnected.

In the BMC Console Redirection area the user can configure the following:

- **Console Speed:** Console Speed default value is 115200.
- **Console Data:** Console data number of bits default value is 8.
- **Console Parity:** Console parity default value is none.
- **Console Stopbits:** Console stop bits default value is 1.
- **Enable hardware flow control:** hardware flow control enable or disable.
- **Enable software flow control:** hardware flow control enable or disable.
- **Log to file:** Log to file enable or disable.
- **Log rotate number:** Log rotate number default value is 20.
- **Log rotate size**: Log rotate size default value is 5.

8.5.2 Console Log

Navigate to **BMC > Console Log** to view BMC Console Log print.
Scroll between pages to view the log history.

8.5.3 Power Control

Navigate to **BMC > Power Control** to view the host power status and update the state of the device.

Power Status indicate:

Power State: Host power up or down
Power Action: N/A

Power Control allows to execute the following:

Click **Power On** to power on the system.
Click **Power Off** to power off the system.
Click **Forceoff** to force power off the system.
Click **Reset** to reset the system.
Click **Cycle** to power cycle the system.

8.5.4 BIOS

Navigate to **BMC > BIOS** to upgrade BIOS on the host.

To upgrade the BIOS, upload a newer version of BIOS image by doing the following:
1. Click **Browse** to navigate to the intended BIOS image file.
2. Click **Start Upgrade**. If the image is correct, a confirmation window will be displayed, asking whether to proceed or not, as shown:

Note: In case the user wants to erase all flash regions tick "Upgrade all flash regions"

8.5.5 USB CDROM

Navigate to **BMC > USB CDROM** to attach or detach Local or Remote image.

To attach the CDROM, upload an image file by doing the following:
1. Select the attachment range **Local Image** or **Remote Image**.
2. Click **Browse** to navigate to the intended CD Rom image.
3. Click **Upload.** If the image is correct, a confirmation window will be displayed, asking whether to proceed or not, as shown:

8.5.6 System Event Log

Navigate to **BMC > System Event Log**
Scroll between pages to view the System Event Log history in the following format:
Date and time, Event, Event Code, Event Description.

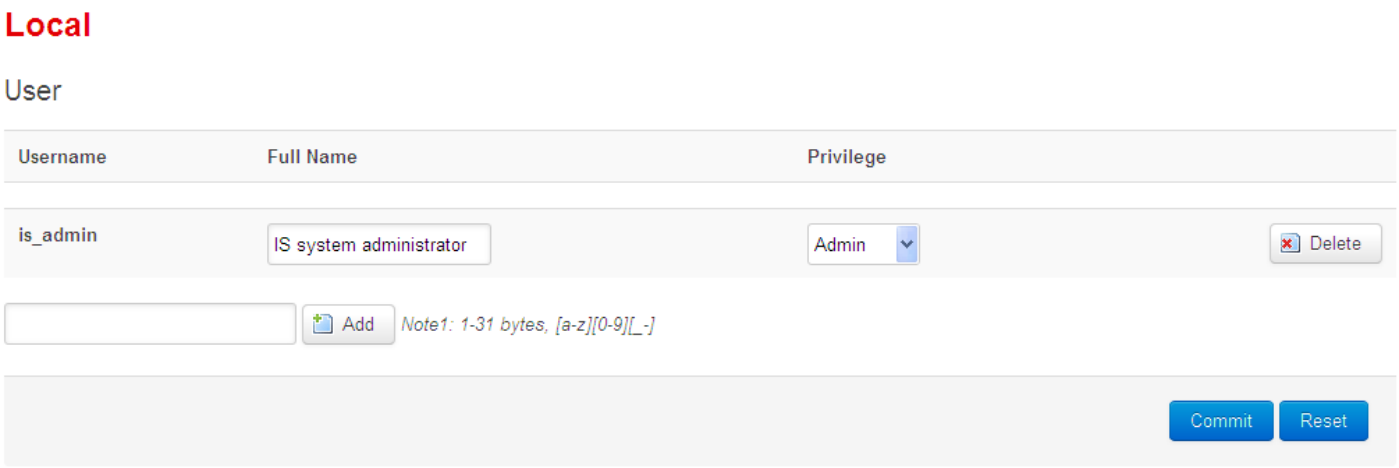
8.6 User

The **User** tab provides access to the following user configuration options:

- **LOCAL**
- **RADIUS**
- **TACACS+**
- **Change Password**

8.6.1 LOCAL

Navigate to **User > LOCAL** to view or modify local users.



Three types of privileges are provided for a local user: **Admin**, **Normal** or **Readonly**.

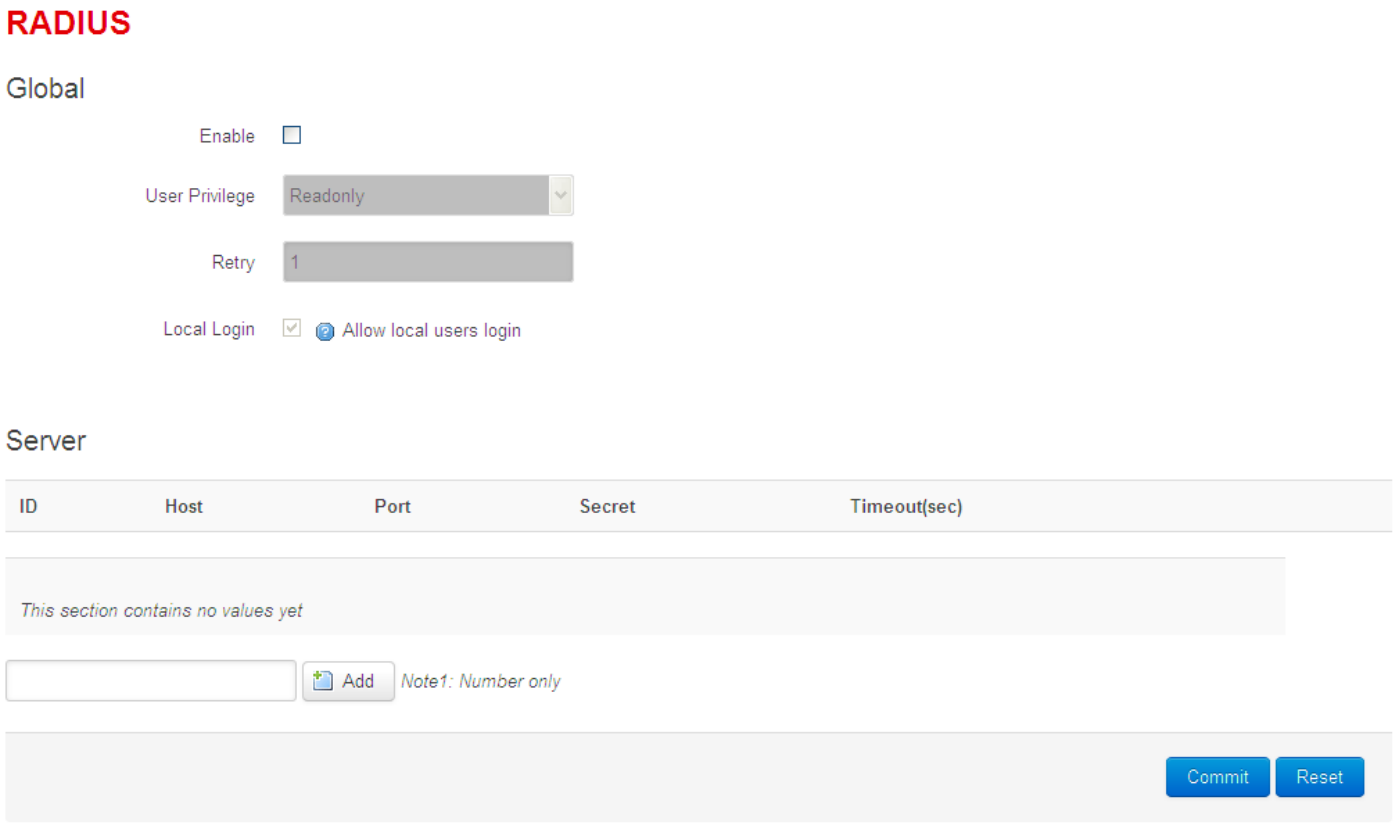
- **Admin:** Full read-write access to all configuration tabs (**Configuration/System/User/ SNMP**); privileges to add, delete, or modify local users on the uBMC. The initial user account **is_admin** is the only administrator account and no other administrator accounts are allowed to be created. This **is_admin** account cannot be deleted, and the privileges cannot be modified.
- **Normal:** Full read-write access to the **Configurations** tab and read-only access to other configuration tabs **(System/User/SNMP).**
- **Readonly:** Read-only access to all configurations.

8.6.2 RADIUS

The uBMC supports RADIUS/TACACS+ remote login. RADIUS and TACACS+ cannot be enabled at the same time. To enable either, the other needs to be disabled first.

RADIUS users share the same privilege level, which can be configured through Web or CLI.

Navigate to **User > RADIUS** to view or modify the RADIUS configuration.



In the **Global** area, the user can configure the following:

- **Enable:** Enable RADIUS remote login.
- **User Privilege:** Set the user privilege. (Readonly)
- **Retry:** Specify how many times to re-send a packet when there is no response from the server.
- **Local Login:** Enable local users' login.

In the **Server** area, the user can configure RADIUS server settings,
including **IP**, **Port**, **Secret** (encrypt/decrypt packets sent/received from the server)
and **Timeout** (value in seconds).

8.6.3 TACACS+

The uBMC supports RADIUS/TACACS+ remote login. RADIUS and TACACS+ cannot be enabled at the same time. To enable either, the other needs to be disabled first.

TACACS+ user or user group privilege can be configured on server side by adding a service tag (default is "silc-system", and this can be configured through Web or CLI, but it can't be the system reserved tags such as slip/ppp/arap/shell/tty-daemon/connection/system/firewall.) to tacacs+ server configuration as below:

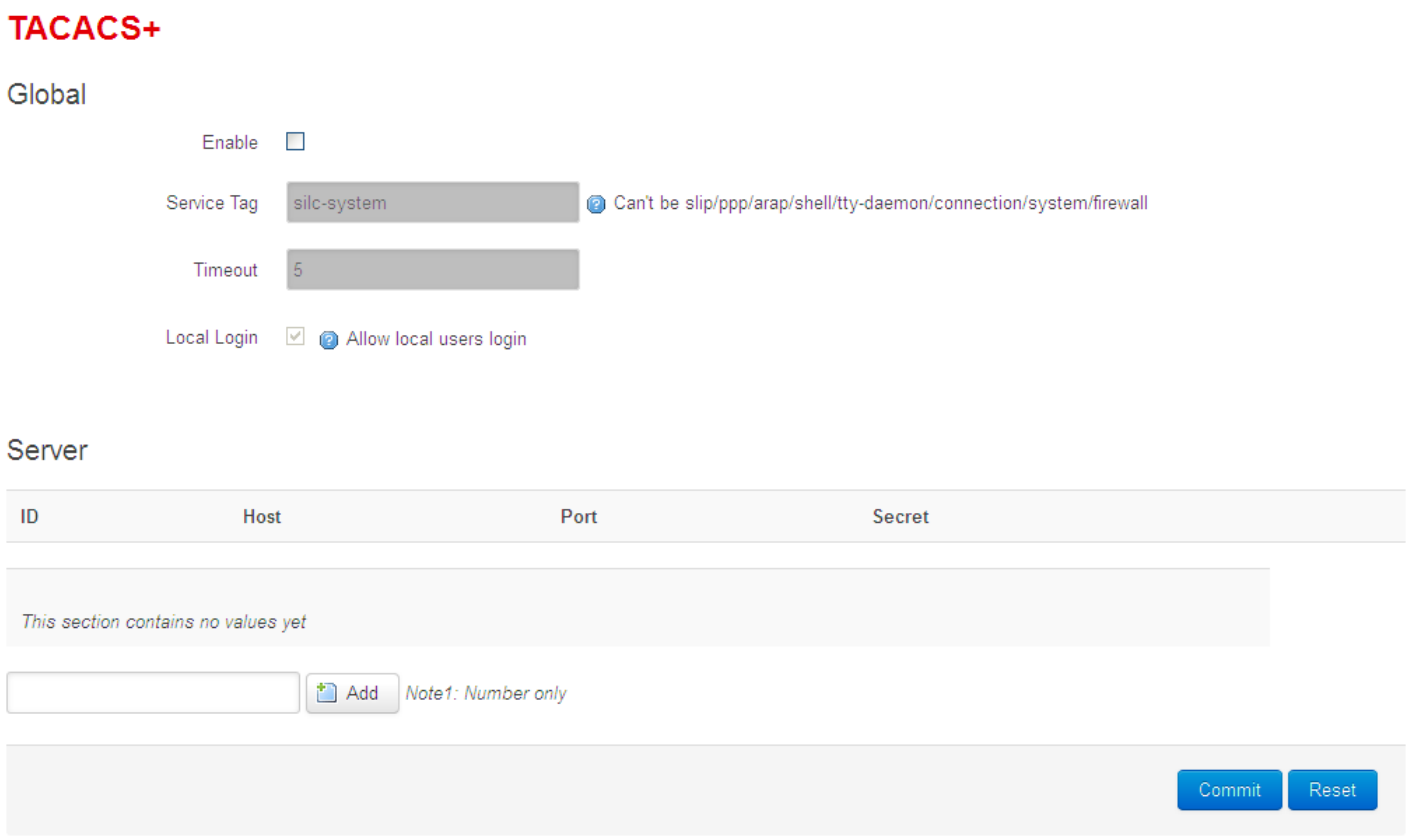
```
service = silc-system {

    # 1: readonly; 5: normal; 10: admin
```

```
        user-privilege = 10
    }
```

And TACACS+ users will be assigned Readonly privilege if the service tag is missing in server configuration.

Navigate to **User > TACACS+** to view or modify the TACACS+ configuration.



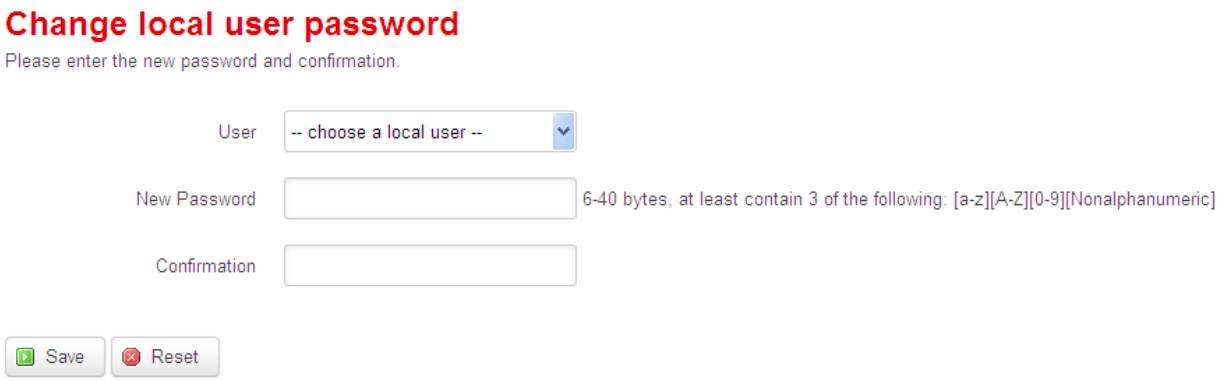
In the **Global** area, the user can configure the following settings:

- **Enable:** Enable TACACS+ remote login.
- **Service Tag:** Configure the service tag.
- **Timeout:** Specify the connection timeout value in seconds.
- **Local Login:** Enable local users' login.

In the **Server** area, the user can configure TACACS+ server settings, including **IP**, **Port**, **Secret** (encrypt/decrypt packets sent/received from the server) and **Timeout** (value in seconds).

8.6.4 Change Password

Navigate to **User > Change Password** to change the local user password.



The **is_admin** user can change the password of all users.

A **Normal** user or a **Readonly** user can only change his own password.

No previous password is required to set a new password.

The password should be 6 to 40 characters, and should contain at least three types of characters from the following character groups:

- [a-z]
- [A-Z]
- [0-9]
- [Non-alpha-numeric]

To Change local user password for the user, that was added in User → Local

1. Select **User** from the drop down menu.
2. Choose the **New Password** per the above guidelines.
3. Retype the password in the **Confirmation** window.
4. Click **Save** button.

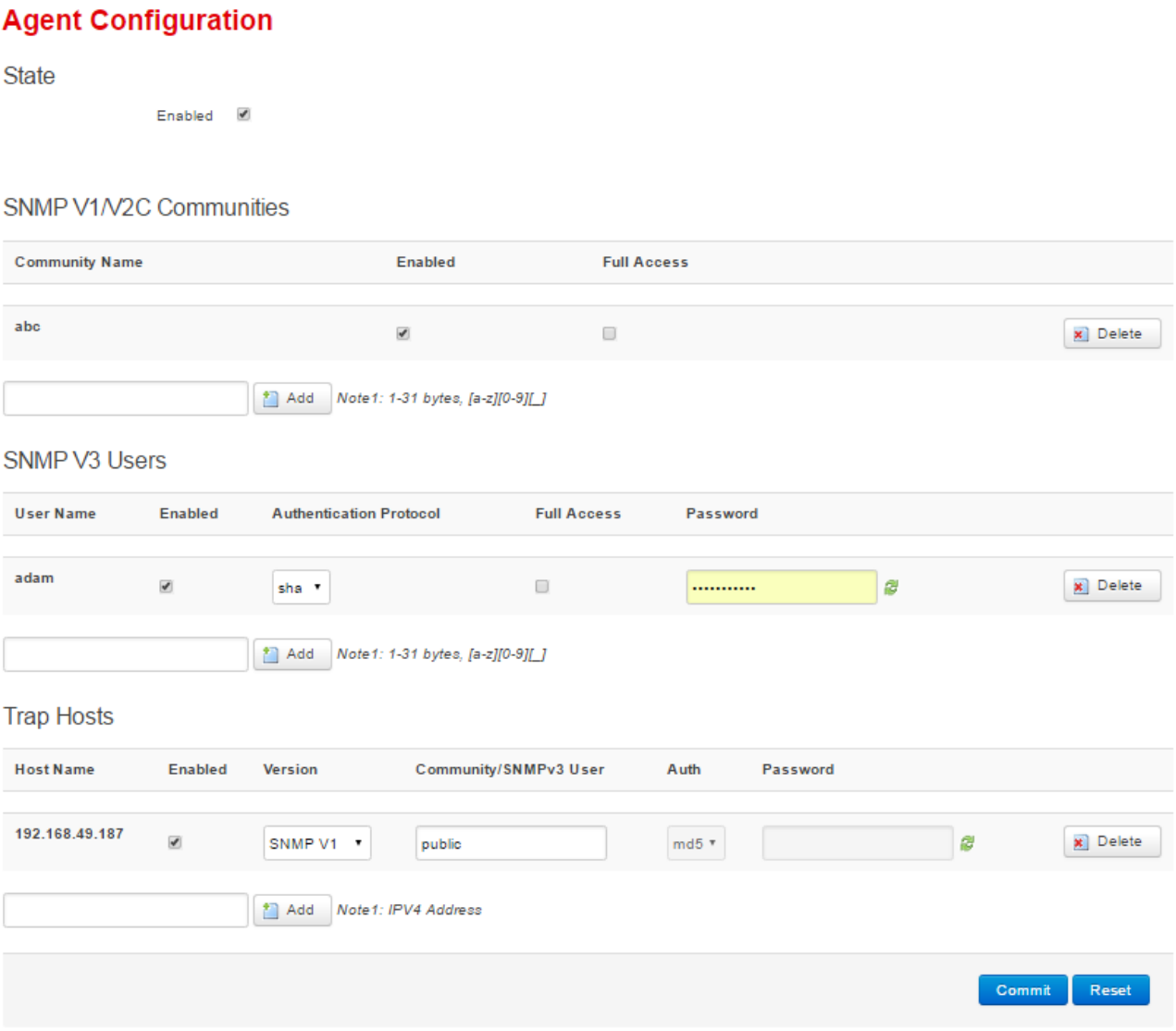
8.7 SNMP

The **SNMP** tab provides access to the following configuration pages:

- **Agent**
- **Mib File**

8.7.1 Agent

Navigate to **SNMP > Agent** to view or modify the Agent Configuration.



In the **State** area, select **Enabled** to enable global SNMP agent configuration.

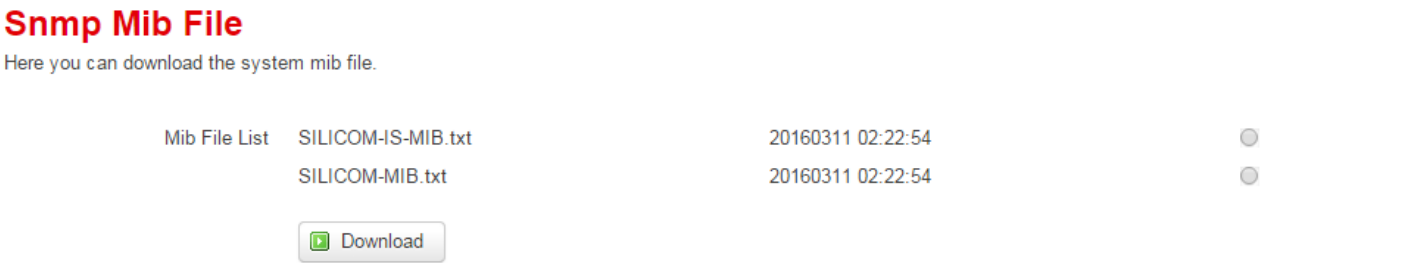
In the **Communities** area and **Users** area, a **Full Access** option is provided.

Select it to grant communities or users write access.

In the **Trap Hosts** area, the user can define the IP address of the SNMP server to which the uBMC will send the SNMP traps.

8.7.2 Mib File

Navigate to **SNMP > Mib File** to download the mib files.



Choose a file and click “Download” to download it.

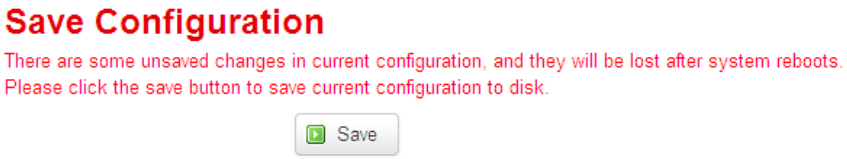
8.8 Logout

To log out from the uBMC Web interface, click the **Logout** tab.

8.9 Save

To save current configurations, click the **Save** tab.

The **Save Configuration** page allows the user to save current configurations to the non-volatile memory so that the configuration will not be lost after the system reboots.



Appendix A Specifications

uBMC **1U host system specifications**

Need to add

Dockings	
Voltage input	
Size	
Operating humidity	
Operating temperature	
Storage temperature	
Fans	
EMC certifications	
MTBF*	

uBMC **1U host system LED and connector specifications**

Need to add

LEDs	
Connectors	

Appendix B Safety precautions

Need to add

Appendix C Copyright notices

NET-SNMP Copyright.

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the

names of its contributors may be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
promote products derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
  brand or product names may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TACACS+ copyright.

Copyright 2000,2001 by Roman Volkov

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The names of its contributors may not be used to endorse or promote
  products derived from this software without specific prior written

permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Next LICENSE text MUST be here:

The MD5 Message-Digest Algorithm was derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm with next copyright:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this

software for any particular purpose. It is provided "as is"
without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

RADIUS copyright.

This code is derived from software contributed to The NetBSD Foundation
by Christos Zoulas.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
      This product includes software developed by the NetBSD
      Foundation, Inc. and its contributors.
4. Neither the name of The NetBSD Foundation nor the names of its
   contributors may be used to endorse or promote products derived
   from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Permission to use, copy, modify, and distribute this software for any
purpose and without fee is hereby granted, provided that this copyright and
permission notice appear on all copies and supporting documentation, the
name of Lars Fenneberg not be used in advertising or publicity pertaining to
distribution of the program without specific prior permission, and notice be
given in supporting documentation that copying and distribution is by
permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this
software for any purpose. It is provided "as is" without express or implied

warranty.
