



Mediatrix Sentinel CS Installation and Activation

Technical Bulletin

2026/06/10

Table of Contents

Host Requirements

Operating System

Software SBC Installation

Launching the Software SBC

Connecting to the SBC via Web Browser

Logging in	7
System Information page	7
Getting an SBC licence key	8
SBC licence key activation	9
Network Status Page	9
SBC Status Page	10

Network Interfaces Configuration – x86

Sentinel CS – x86 virtual environment	11
Enabling the second network interface in Ubuntu	12

Network Interfaces Configuration – ARM

Notes on the Sentinel Mini	13
Setting the Uplink interface static IP	14
Setting the Uplink interface to DHCP mode	14
Setting the Lan1 interface static IP	14
Setting the Lan1 interface to DHCP mode	14
Restoring a network interface	15
Associating a VLAN to an interface	16

SSH port notes

Advanced operations

Stopping the Software SBC service	17
Systemctl commands	17
Get DGW console output (troubleshooting)	17
CLI	17

Linux Operating System

Supported Linux Distributions	18
Linux OS support and general information	18
Minimum Linux host OS requirements	18

Copyright Notice

Host Requirements

Resource	Minimum requirements
Processor type	64-bit Intel or AMD CPU with support for hardware virtualization (VT-x) enabled
Number of CPU Cores	1 vCPU minimum (estimate 300-400 simultaneous calls per vCPU with media relay)
Memory	2 GB
Disk Space	16GB recommended (4GB initial image + growing space)
Network interfaces	1 interface minimum (e1000 driver or another high-performance virtualized driver) 2 network cards recommended for network demarcation
Environment	Bare metal, VMWare, Hyper-V, Azure, Amazon, Google Cloud, VirtualBox, KVM/Qemu

Operating System

The Mediatrix Sentinel SBC requires a recent, supported Linux distribution with long-term security updates available.

M5 uses and recommends Rocky Linux 9, Ubuntu 24.04 LTS, and Debian 12/13, these distributions feature a stable (non-rolling) release and have an official long-term support, plus an Extended Security Maintenance that goes beyond 2030.

It should also work on other distributions using "systemd", such as Centos Stream 9/10 and openSUSE Leap 16.1, however these are not officially tested by M5 for GA purposes.

Ubuntu is readily documented and pre-built images are officially available on multiple cloud providers such as Amazon, Azure, Hetzner Cloud and others.

- Amazon AWS: <https://aws.amazon.com/marketplace/pp/prodview-jg5ptpxgyzhje>
- Azure: https://marketplace.microsoft.com/en-us/product/canonical.ubuntu-26_04-lts
- Google cloud: <https://console.cloud.google.com/marketplace/browse?q=ubuntu%20pro%20lts>
- Hetzner: <https://bizanosa.com/deploy-ubuntu-hetzner-cloud-login-ssh/>
- Ubuntu (26.04 - Resolute): <https://cloud-images.ubuntu.com/resolute/current/>
- Ubuntu (24.04 - Noble): <https://cloud-images.ubuntu.com/noble/current/>

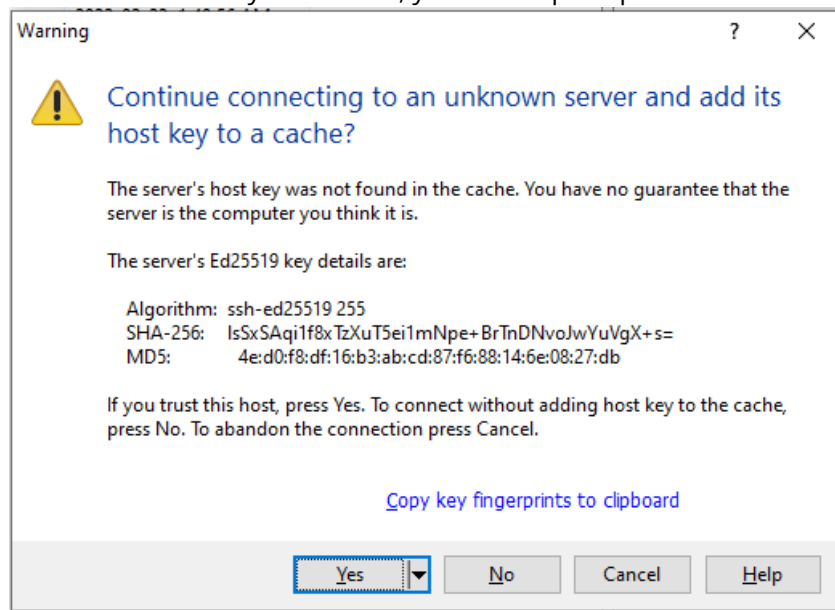
The installation procedure for VMWare is also documented on the internet:

<https://blog.eldernode.com/install-ubuntu-20-04-lts-server-on-vmware/>

Software SBC Installation

Steps:

- Download the installation file from <https://liquidfiles.media5corp.com/>
 - **x86-64:** MediatrixSentinelCS_x86-64_Dgw_50.2.3182_SBCX-MX-D2000-178.bin.bash
 - **ARM32:** MediatrixSentinelCS_arm32_Dgw_50.2.3182_SBCX-MX-D2001-55.bin.bash
- Connect to the VM using an SCP client (e.g. WinSCP):
 - File Protocol: SCP
 - Host Name: The IP address of the VM
 - If it is the first time you connect, you will be prompted to add the host key to the cache



- Connect to the VM using an SSH client:
 - Host Name: The IP address of the VM
 - Enter administrative mode: "sudo su -" (or simply "su").

```
vmuser@vmserver:~$
vmuser@vmserver:~$ sudo su -
[sudo] password for vmuser:
root@vmserver:~#
```

- Go to the /home/vmuser directory and verify if the installation files are present:


```
root@vmserver:~# cd /home/vmuser
root@vmserver:/home/vmuser# ls -l
```

- Make the script executable and run it:


```
chmod a+x MediatriceSentinelCS_*.bin.bash
```

X86-64:

```
./MediatriceSentinelCS_x86-64_Dgw_49.5.3041_SBCX-MX-D2000-163.bin.bash
```

ARM32:

```
./MediatriceSentinelCS_arm32_Dgw_49.5.3041_SBCX-MX-D2001-40.bin.bash
```

- You should see the following result:

INFO: DGW will be installed from embedded load.

3+0 records in

3+0 records out

3 bytes copied, 3.4764e-05 s, 86.3 kB/s

6323+1 records in

6323+1 records out

25902919 bytes (26 MB, 25 MiB) copied, 0.618489 s, 41.9 MB/s

INFO: Updating /opt/m5t/sbc/dgw/bootstrap.sh

from

/opt/m5t/sbc/dgw/mitosrfs.2/muse/bootstrap.sh.

INFO: Executing the Sentinel CS installation script to complete the installation.

INFO: Adding the Sentinel CS to systemd as sbc.service.

Created symlink /etc/systemd/system/multi-user.target.wants/sbc.service

→

/etc/systemd/system/sbc.service.

INFO: Starting the Sentinel CS through systemd: systemctl start sbc.service.

INFO: Sentinel CS installed successfully.

Launching the Software SBC

The SBC runs through the "systemd" system and service manager that is provided by all standard Linux distributions.

After installation, it is automatically started and set to run on every boot.

You can use the "systemctl" command to see the status of the service (sbc):

```
systemctl status sbc
```

You should get the following result (press "q" to exit the status):

```
● sbc.service - Sentinel CS (DGW/SBC) service
   Loaded: loaded (/etc/systemd/system/sbc.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-12-03 01:20:47 UTC; 49s ago
     Main PID: 1578 (start_dgw.bash)
        Tasks: 89 (limit: 2280)
       Memory: 21.0M
      CGroup: /system.slice/sbc.service
[...]
```

```
Dec 03 01:20:53 ubuntu-2gb-ash-2 dgw[1936]: *****
Dec 03 01:20:53 ubuntu-2gb-ash-2 dgw[1936]: ***** Boot up completed *****
Dec 03 01:20:53 ubuntu-2gb-ash-2 dgw[1936]: *****
```

You can also check the syslog with commands like:

```
tail -n 100 /var/log/syslog |grep dgw
journalctl -u sbc -e --no-pager
```

Connecting to the SBC via Web Browser

Logging in

Using a web browser, connect to the IP address of your Virtual machine, and login with the username "admin" and the password "administrator".



✚ Please enter your username and password

User Name:

Password:

System Information page



☒ System
 ☐ Network
 ☐ SBC
 ☐ Management
 ☐ Reboot

✚ Information

Current Status	
Device Identification:	Mediatrix Sentinel CS
Firmware:	Dgw 49.5.3041
Profile:	SBCX-MX-D2000-163
MAC Address:	080027b8f6bf
Serial Number:	0000000000000000
UUID:	4dd2c0b7-898b-6b47-b531-51ffc0f750a5
Storage Memory (in use/total):	4.1 GB / 8 GB
Volatile Memory (in use/total):	182.3 MB / 2 GB
System Uptime (D:HH:MM:SS):	0:00:05:22
System Time (DD/MM/YYYY HH:MM:SS):	08/05/2025 11:16:15

Licences	
No SBC licence found. The demo mode is limited to 3 SBC sessions .	

Activate Licence	
Licence Key:	

Getting an SBC licence key

The Mediatrix Sentinel CS is licenced per session, based on the hardware identification of the Virtual machine or Cloud instance.

The system UUID must be provided to M5 to generate a licence key:

- If you already installed the Sentinel CS software, the UUID is available on the System/Information page:

Information

Current Status	
Device Identification:	Mediatrix Sentinel CS
Firmware:	Dgw 49.5.3041
Profile:	SBCX-MX-D2000-163
MAC Address:	080027b8f6bf
Serial Number:	0000000000000000
UUID:	4dd2c0b7-898b-6b47-b531-51ffc0f750a5
Storage Memory (in use/total):	4.1 GB / 8 GB

- The UUID can be obtained via Linux command line:

```
# cat /sys/class/dmi/id/product_uuid
d926ea5e-7401-4608-9dbc-1c7003ba685b
```

- It is also recommended to include the MAC address of the network interfaces, available with the "ip addr" command:

```
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 96:00:01:42:52:23 brd ff:ff:ff:ff:ff:ff
    altnam enpls0
    inet 5.161.64.241/32 metric 100 scope global dynamic eth0
    valid_lft 79625sec preferred_lft 79625sec
```

SBC licence key activation

Steps:

- Scroll down to “Activate Licence” menu in the “System/Information” page
- Paste the licence key provided by M5
- Click “Apply”

Activate Licence	
Licence Key:	3bGljZW5zZV90eXBIPVNiY1Nlc3Npb25z

- The licence is automatically activated, and the updated information will be displayed:

Licences
SBC Licence for 30 concurrent sessions

Network Status Page



☐ System
 ☒ Network
 ☐ SBC
 ☐ Management
 ☐ Reboot

Status

Interfaces Status					
Name	Link	IP Address	Default Router	VLAN Override	Status
Lan1				Disable	Invalid Configuration
Uplink	enp0s3	172.16.10.156/24		Disable	Active

Host Status	
General Configuration:	
IPv4 Automatic Configuration Interface:	Uplink
IPv6 Automatic Configuration Interface:	UplinkV6
Host Name Configuration	
Host Name:	sentinelcs
Domain Name:	lan
Default Gateway Configuration	
IPv4 Default Gateway:	172.16.10.254
IPv6 Default Gateway:	0.0.0.0
DNS Configuration	
Primary DNS:	127.0.0.53
SNTP Configuration	
Primary SNTP:	ntp.media5corp.com:123

Notes:

- By default, the Software SBC configures the network interfaces to automatically use the Linux host network configuration (IpSystem).
- If there is just one network interface (eth0), and no eth1, an "Invalid Configuration" message will be displayed for Lan1, which is normal since the SBC cannot find a second interface

SBC Status Page

Verify that the Signaling Interface "uplink_s" is Active.

Note: lan1_s will be down if there is no eth1.



☐ System
 ☐ Network
 ☒ SBC
 ☐ Management
 ☐ Reboot

Status
 Configuration
 Rulesets
 Live Calls
 Running Config
 Events
 Registration

Status

Show Call Agent Rulesets

Configuration Modified:	no
-------------------------	----

Call Agent Name	Signaling Interface	Media Interface	Peer	State
registration_ca	loop_s	loop_m	127.0.0.1:5060	Active

Routing Rulesets	Parameters
Priority Name	

Signaling Interface								
Name	Network Name	Network Address	Port	Secure Port	Allowed Transports	Tls Mode	Public Address	State
loop_s	Loop	127.0.0.1	0	0	All	Client		Active
lan1_s	Lan1		0	0	All	Client		Network Down
uplink_s	Uplink	172.16.10.156	0	0	All	Client		Active

Media Interface					
Name	Network Name	Network Address	Port Range	Public Address	State
loop_m	Loop	127.0.0.1	20000-49999		Active
lan1_m	Lan1		20000-49999		Network Down
uplink_m	Uplink	172.16.10.156	20000-49999		Active

Registration Agent Status					
User Name	Friendly Name	Domain	Contact	Registration Type	State

Network Interfaces Configuration – x86

On most virtualization and cloud hosting there's only one network interface by default. Lan1 configuration status will be marked as invalid, which is the normal behavior.

If another interface is added, Lan1 will automatically pick up the new configuration upon the SBC restart.

Sentinel CS – x86 virtual environment

When creating a second interface, make sure that:

- 1) Adapter type is set to E1000
- 2) Each card is bound to a different vSwitch
- 3) The MAC address for eth0 is lower than the one for eth1. By default eth0 will be associated to the Uplink interface and eth1 to LAN1.

VMware specific notes:

- Check which Virtual NIC is used (E1000 or VMXNET3):
 - Usually, ova files are shipped with the E1000 driver, for platform compatibility purposes (VMWare Workstation, VirtualBox, etc)
 - On dedicated ESXi systems, VMXNET3 is used by default
 - Make sure that both interfaces are set to the same driver, or the cards order might be reversed
- <https://kb.vmware.com/s/article/1001805>

Enabling the second network interface in Ubuntu

By default, Ubuntu only activates the link on interfaces configured in netplan, the static IP must be set there. On DGW Network, leave the interface as ipSystem.

To activate the second network interface, edit the netplan file and add "eth0:" with "dhcp4: false".

- Ubuntu 24.04/26.04: /etc/netplan/50-cloud-init.yaml

The configuration for the Uplink interface (corresponding to ETH0) should be done using the DGW Network interface.

```
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: false
    eth1:
      addresses:
        - 192.168.0.10/24
      nameservers:
        search: [mydomain, otherdomain]
        addresses: [192.168.0.1, 1.1.1.1]
      routes:
        - to: default
          via: 192.168.0.1
```

Notes:

- Use the command "nano /etc/netplan/50-cloud-init.yaml" to edit the file. When ready to save, press CTRL-X.
- To make sure the network is in a sane state:
 service dgw stop
 netplan apply
 service dgw start

Network Interfaces Configuration – ARM

Notes on the Sentinel Mini

- Uplink interface is in DHCP mode by default
- Lan1 interface is set to a static IP by default, 192.168.0.10/24
- All commands must be executed as root, default password is administrator:

```
sudo su -  
[sudo] password for admin:
```

- Configuration type for the interfaces on the SBC must be set to IpSystem:

Network Interface Configuration					
Name	Link	Type	Static IP Address	Static Default Router	Activation
Lan1	enP2p33s0	IpSystem (IPv4 System)			Enable
Uplink	enp1s0	IpSystem (IPv4 System)			Enable

- Uplink ETH is next to the USB A port, the second ETH port is Lan1



Setting the Uplink interface static IP

```
nmcli con mod uplink ipv4.addresses 10.10.0.10/24
nmcli con mod uplink ipv4.gateway 10.10.0.1
nmcli con mod uplink ipv4.dns 10.10.0.1
nmcli con mod uplink ipv4.method manual
nmcli con up id 'uplink'
```

Replace the IPs for desired ones.

Setting the Uplink interface to DHCP mode

```
nmcli con mod uplink ipv4.method auto
nmcli con mod uplink ipv4.gateway ""
nmcli con mod uplink ipv4.addresses ""
nmcli con mod uplink ipv4.dns ""
nmcli con up id 'uplink'
```

Setting the Lan1 interface static IP

```
nmcli con mod lan1 ipv4.addresses 172.16.0.10/24
nmcli con mod lan1 ipv4.gateway 172.16.0.254
nmcli con mod lan1 ipv4.dns 172.16.0.254
nmcli con mod lan1 ipv4.method manual
nmcli con up id 'lan1'
```

Replace the IPs for desired ones.

Setting the Lan1 interface to DHCP mode

```
nmcli con mod lan1 ipv4.method auto
nmcli con mod lan1 ipv4.gateway ""
nmcli con mod lan1 ipv4.addresses ""
nmcli con mod lan1 ipv4.dns ""
nmcli con up id 'lan1'
```

Restoring a network interface

If an interface is deleted by accident, it will be displayed as “Wired Connection” when executing the **“nmcli connection show”** command.

Example, missing Uplink interface:

```
# nmcli connection show
NAME          UUID                                  TYPE    DEVICE
lan1          c6c993d9-3180-4eb5-a81f-49b6e270f42f ethernet enP2p33s0
Wired connection 1 6acd534f-8d1c-397f-9921-6595dd73be17 ethernet enp1s0
```

Use the **“nmcli con add”** command to restore back the missing interface back, then **“nmcli connection delete”** to delete the wired connection.

Example, Uplink interface:

```
nmcli con add type ethernet con-name 'uplink' ifname enp1s0 ipv4.method auto
nmcli con up id 'uplink'
```

Delete the Wired connection:

```
nmcli connection delete Wired\ connection\ 1
```

Execute the **“nmcli connection show”** command to validate the results:

```
# nmcli connection show
NAME  UUID                                  TYPE    DEVICE
lan1   c6c932d9-3580-4fb5-a81r-49b5e279f42f ethernet enP2p33s0
uplink abze09z3-fefc-4saf-bc2c-0bd9bf1f4f85 ethernet enp1s0
```

Associating a VLAN to an interface

Example, VLAN ID 11 on Uplink interface with static IP 192.168.88.199:

```
nmcli con add type vlan ifname VLAN11 dev enp1s0 id 11 ipv4.method manual ipv4.addresses 192.168.88.199/24
nmcli con up id 'vlan-VLAN11'
systemctl sbc restart
```

Once configured with nmcli commands, assign the new VLAN interface on DGW:

Network Interface Configuration						
Name	Link	Type	Static IP Address	Static Default Router	Activation	
Lan1	enP2p33s0 ▾	IpSystem (IPv4 System) ▾			Enable ▾	—
Uplink	VLAN11 ▾	IpSystem (IPv4 System) ▾			Enable ▾	—

SSH port notes

The default ssh port is 2255 in the Sentinel CS, to avoid conflicts with the main VM ssh port. This is configurable in both Linux and DGW, so it can be changed according to each deployment requirements. When using Amazon, or other cloud services, by default ssh connections are only allowed through port 22, and private-key authentication is required.

Advanced operations

Stopping the Software SBC service

When stopping the Software SBC (sbc service), the following command must be used:

```
service sbc stop;netplan apply
```

The "netplan apply" is required in case the service attempts to remove the main IP address.

Systemctl commands

To disable or enable the service at boot, or check the status, systemctl command must be used:

```
systemctl disable sbc  
systemctl enable sbc  
systemctl is-active sbc.service  
systemctl is-enabled sbc.service
```

Get DGW console output (troubleshooting)

```
# Dump logs in a file  
journalctl -u sbc -a > logs.txt  
# Or "follow" the logs for live troubleshooting  
journalctl -u sbc -f
```

CLI

For TAC troubleshooting:

- If the network configuration has errors, the CLI can be launched manually (localhost should always be running):

```
ssh admin@localhost -p 2255
```
- If Hoc.ManagementInterface has been set to a specific interface, and the network is no longer available:

```
chroot /proc/$(pidof main.exe)/root /muse/persistent/Components/CP_Cli/bin/Cli.exe
```

Linux Operating System

NOTE: M5 may not support an operating system for various reasons, including discontinued support from the software vendor, lack of availability with certain products, or other reasons.

Supported Linux Distributions

- Rocky Linux 9
- Ubuntu 24.04 LTS

M5 uses and recommends these two distributions, both feature a stable (non-rolling) release and have an official long-term support, plus and Extended Security Maintenance that goes beyond 2030.

Specific Linux distribution best practices must be followed.

Linux OS support and general information

- M5 supplies reference guides to help Ubuntu users to handle specific use cases.
- Ubuntu support sites:
 - www.ubuntu.com
 - askubuntu.com/
 - www.canonical.com
- Rocky Linux support sites:
 - rockylinux.org/support/
 - wiki.rockylinux.org/rocky/support/

Minimum Linux host OS requirements

- systemd
 - multi-user.target
 - network-online.target
- bash and user commands
- system commands:
 - chroot
 - chmod
 - mount and umount
 - dd
 - sleep
 - tar

- Valid /etc/resolv.conf file or symlink with actual DNS info (For IpSystem network connection type)
- Linux kernel:
 - tmpfs filesystem support (CONFIG_TMPFS=y)
 - sysfs filesystem support (CONFIG_SYSFS=y)
 - proc filesystem support (CONFIG_PROC_FS=y, CONFIG_PROC_SYSCTL=y)
 - devpts filesystem support
 - IPv4 (CONFIG_INET=y)
 - Unix sockets (CONFIG_UNIX=y)
 - Preemption (CONFIG_PREEMPT=y)
 - TTY (CONFIG_TTY=y)
 - PTYS (CONFIG_UNIX98_PTYS=y)
 - Inotify (CONFIG_INOTIFY_USER=y)

Copyright Notice

Copyright © 2026 M5 Technologies.

This document contains information that is proprietary to M5 Technologies.

M5 Technologies reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by M5 Technologies.

M5 Technologies reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



130, rue Sauvé
Sherbrooke (Québec)
J1L 0A7 Canada
m5technologies.com