Secure Router Manual

Netgate 8300

Aug 15, 2024

OUT OF THE BOX

This Quick Start Guide covers the first time connection procedures for the Netgate® 8300 Secure Router and also provides information necessary to keep the appliance up and running.

CHAPTER ONE

GETTING STARTED

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   Note: Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.
3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

CHAPTER

TWO

INPUT AND OUTPUT PORTS

2.1 Front Panel

The front panel of the Netgate 8300 contains several items of interest for connecting to and managing the device.

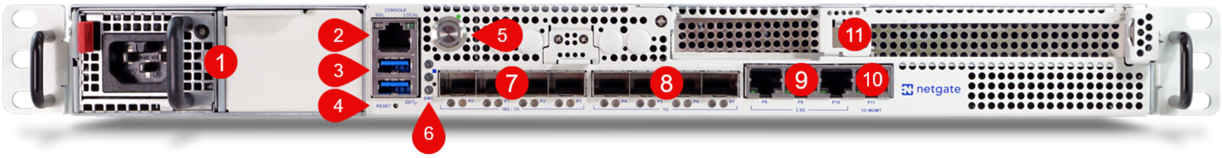


Fig. 1: Front view of the Netgate 8300 Security Gateway with key items numbered

The items below are marked with numbers on figure *Front view of the Netgate 8300 Security Gateway with key items numbered*:

Item	Description
1	Power Supply Unit (PSU) Bays
2	Serial Console (*RJ45*)
3	2x USB 3.0 Port
4	Reset Button
5	ACPI Power Button - Graceful shutdown, hard power off (Hold 10s), power on
6	*Status LEDs*
7	10G/1G SFP+ *Networking Ports*
8	1G SFP+ *Networking Ports*
9	2.5G RJ45 *Networking Ports*
10	1G IPMI Management Port (P11, *Intelligent Platform Management Interface (IPMI)*)
11	Add-on Expansion Card Slots

Power Supply Unit (PSU) Bays (1)

The chassis contains two power supply unit bays located on the far left of the front side. The PSUs are hot swappable and the unit can operate with one or both PSUs connected to line power.

The Netgate 8300 BASE unit ships with one power supply, the Netgate 8300 MAX unit ships with dual power supplies. Additional power supplies are available. A second PSU can be added to the BASE model later by removing the blank panel cover.

Each PSU is 500W with 110V/240V AC input. It contains a standard IEC320-C16 (3-pin) power receptacle which accepts a standard IEC320-C15 power plug.

Serial Console Port (2)

Clients can access the serial console using the *RJ45* “Cisco” style console port with a separate cable and USB serial adapter or client hardware port.

> **Note:** The RJ45 Serial Console port is only for use with the Serial Console. It cannot be used for any other purpose.

2x USB 3.0 Ports (3)

USB ports on the device can be used for a variety of purposes.

The primary use for the USB ports is to install or reinstall the operating system on the device. Beyond that, any purposes are left to administrators to configure and utilize.

Reset Button (4)

The Reset Button acts as a standard hardware reset button and immediately resets the hardware when pressed.

ACPI Power Button (5)

The large round lighted Power Button behaves the same as a typical ACPI power button.

If the device is powered on and running, pressing the button immediately performs a graceful shutdown and the system enters a standby state.

If the system is in a powered off or standby state, pressing the power button immediately powers on the device and starts the boot process.

If the system is unresponsive, holding in the power button for 10 seconds will forcefully power off the device. Press the power button again to turn it back on.

Status LEDs (6)

The status LEDs, including the backlight on the power button, indicate various status information for the device. The power button LED and the first two LEDs from top to bottom are for OS status, while the bottom LED is for the status of the baseboard management controller (BMC).

See *Status LEDs* for information on interpreting the meaning of different LED states.

10G/1G SFP+ Networking Ports (7)

This group of four ports labeled P0-P3 are *10G/1G SFP+ Networking Ports*.

1G SFP+ Networking Ports (8)

This group of four ports labeled P4-P7 are *1G SFP+ Networking Ports*.

2.5G RJ45 Networking Ports (9)

This group of three ports labeled P8-P10 are *2.5G RJ45 Networking Ports*.

1G IPMI Management Port (10)

The rightmost RJ45 port labeled P11 is the 1G MGMT port dedicated to IPMI. See *Intelligent Platform Management Interface (IPMI)* for details on how to access IPMI.

> **Note:** This dedicated IPMI management port is not visible to or usable by the operating system.

Add-on Expansion Card Slots (11)

These are expansion slots and covers which may house additional add-on cards such as for network interfaces. See *Add-On Expansion Card Installation* for installation information.

There are two available expansion slots:

- 1x PCIe 3.0 x8 LP (Low Profile) slot which supports half-length low profile cards.

This slot has a PCIe-LP connector which is PCIe x16 but only wired for PCIe x8. While the slot supports PCIe x16 half length cards, only 8 lanes function.

- 1x PCIe 4.0 x16 slot which supports full-height three-quarter length cards.

  This x16 PCIe slot can supply a maximum of 75W directly.

Note: The power draw of standard 25-100 Gbit/s network interface cards will NOT exceed the standard 75W slot rating.

2.1.1 Networking Ports

The sections on the front of the device numbered **7**, **8**, and **9** in *Front view of the Netgate 8300 Security Gateway with key items numbered* contain the network interfaces. These ports are labeled **P0** through **P10** on the device and are grouped by speed.

Table 1: Netgate 8300 Secure Router Network Interface Layout

Label	Bus Address	Linux Label	TNSR Label	Port Type	Port Speed
P0	0000:f4:00.0	eno2	TwentyFiveGigabitEthernetf4/0/0	SFP+	10 Gbps/1 Gbps
P1	0000:f4:00.1	eno3	TwentyFiveGigabitEthernetf4/0/1	SFP+	10 Gbps/1 Gbps
P2	0000:f4:00.2	eno4	TwentyFiveGigabitEthernetf4/0/2	SFP+	10 Gbps/1 Gbps
P3	0000:f4:00.3	eno5	TwentyFiveGigabitEthernetf4/0/3	SFP+	10 Gbps/1 Gbps
P4	0000:f4:00.4	enp244s0f4	TwentyFiveGigabitEthernetf4/0/4	SFP+	1 Gbps
P5	0000:f4:00.5	enp244s0f5	TwentyFiveGigabitEthernetf4/0/5	SFP+	1 Gbps
P6	0000:f4:00.6	enp244s0f6	TwentyFiveGigabitEthernetf4/0/6	SFP+	1 Gbps
P7	0000:f4:00.7	enp244s0f7	TwentyFiveGigabitEthernetf4/0/7	SFP+	1 Gbps
P8	0000:0d:00.0	eno1	TwoDotFiveGigabitEthernetd/0/0	RJ45	2.5 Gbps
P9	0000:0b:00.0	ens9	TwoDotFiveGigabitEthernetb/0/0	RJ45	2.5 Gbps
P10	0000:09:00.0	ens8	TwoDotFiveGigabitEthernet9/0/0	RJ45	2.5 Gbps

2.1.2 Networking Ports with Add-on Cards

There are two add-on expansion card slots on the Netgate 8300 device and they can both be populated with network cards, for a total of either two or four additional network ports.

The following table shows interface information for a Netgate 8300 containing an E810-XXV card with 2x 25 Gbit/s ports in the x8 half height slot and an E810-C card with 2x 100 Gbit/s ports in the x16 full height slot.

Table 2: Netgate 8300 Secure Router Add-On Network Interfaces

Bus Address	Linux Label	TNSR Label	Port Type	Port Speed
0000:03:00.0	enp3s0f0	TwentyFiveGigabitEthernet3/0/0	SFP	25 Gbit/s
0000:03:00.1	enp3s0f1	TwentyFiveGigabitEthernet3/0/1	SFP	25 Gbit/s
0000:15:00.0	ens6f0	HundredGigabitEthernet15/0/0	QSFP	100 Gbit/s
0000:15:00.1	ens6f1	HundredGigabitEthernet15/0/1	QSFP	100 Gbit/s

2.2 Status LEDs

The Netgate 8300 has two groups of status LEDs: Three LEDs (including the power button) for the operating system status, and one LED for the baseboard management controller (BMC) status.

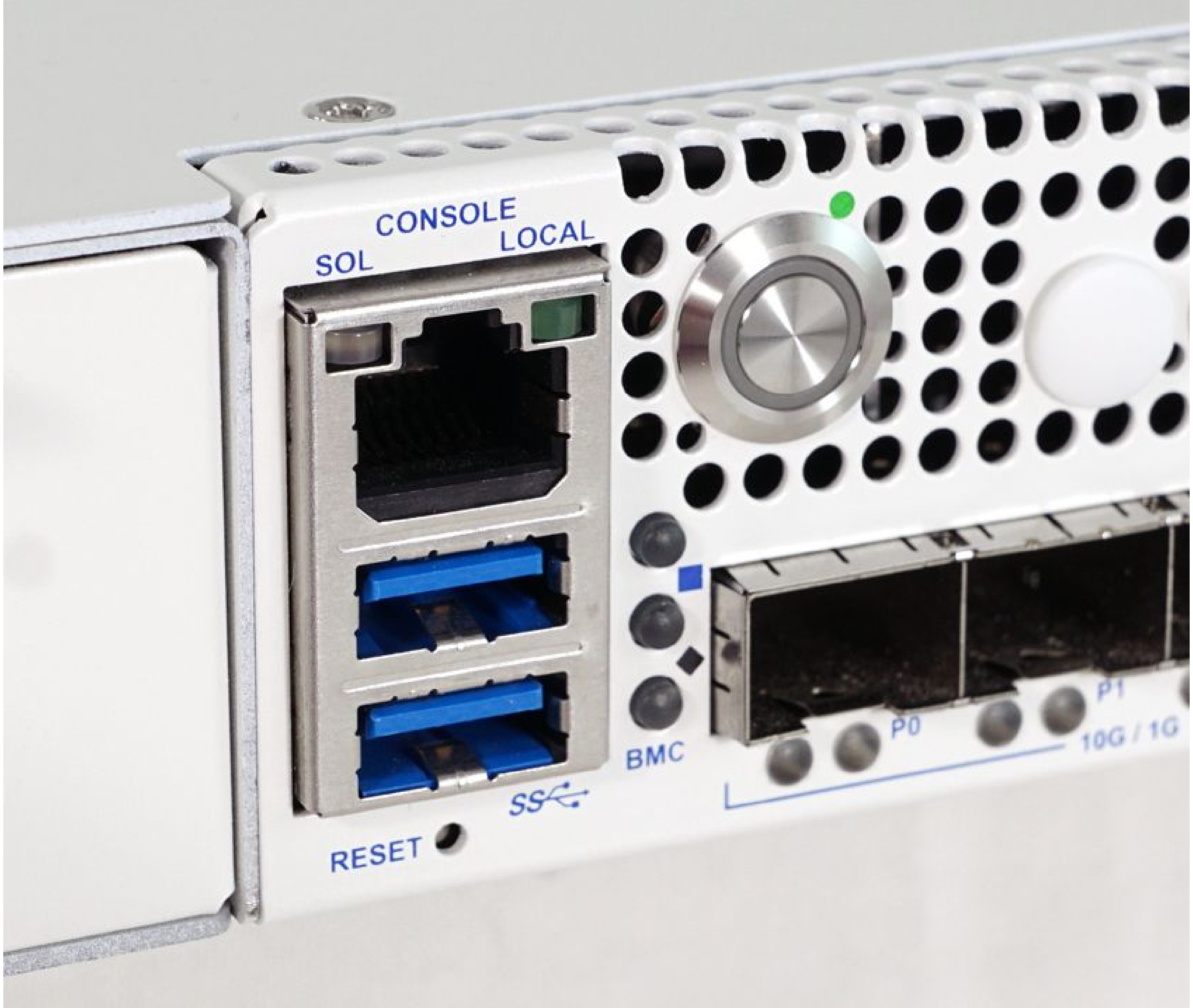


Fig. 2: Close-up view of the Netgate 8300 Security Gateway Status LEDs

The Operating System status LEDs are labeled with shapes which correspond to each LED: Green Circle, Blue Square, and Black Diamond. The BMC status LED is labeled "BMC".

2.2.1 OS Status LED Patterns

Description	LED Pattern
Standby	Circle pulsing amber
Power Applied	Circle solid amber
BIOS Booting	Circle flashing green
Running	Circle solid green

2.2.2 BMC Status LED Patterns

Description	LED Pattern
BMC Power Applied	BMC solid amber
BMC OS Booting	BMC flashing blue
BMC Boot Completed/Ready	BMC solid blue

2.2.3 Power Supply Unit LED Patterns

Each power supply has a status LED in the upper right corner (not pictured).

Description	LED Pattern
Power Applied + Power On	PSU solid green
Power Applied + Power Off	PSU flashing green
Power Loss to all PSUs	PSU off
Power Loss to one PSU[1]	PSU flashing amber
Warning Event[2]	PSU flashing alternating amber and green
Critical Event[3]	PSU solid amber

PSU LED Notes

2.3 Rear Panel

The rear panel of the device has items which are not meant to be accessed as often as the front, as the device is intended to be mounted in a rack.

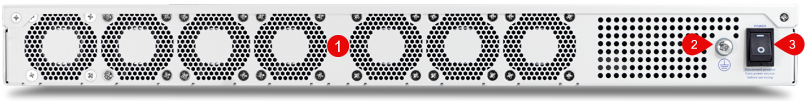


Fig. 3: Rear view of the Netgate 8300 Security Gateway with key items numbered

[1] When multiple PSUs are installed.

[2] PSU continues operating during warning events. Warning events include: High temperature, power level higher than expected, current higher than expected, fan operating slower than expected.

[3] Critical events cause a PSU to shut down. Critical events include: PSU failure, output over current protection, output over voltage protection, fan failure.

The items below are marked with numbers on figure *Rear view of the Netgate 8300 Security Gateway with key items numbered*:

Item	Description
1	Fan exhaust grills
2	Ground connection
3	Power switch

CHAPTER

THREE

CONNECTING TO THE CONSOLE PORT

There are times when directly accessing the console is required. Perhaps GUI or SSH access has been locked out, or the password has been lost or forgotten.

There are multiple ways to access the console on the **Netgate 8300**:

- IPMI Web Browser Serial Console
- Serial over LAN (SOL) via `ipmitool`
- Using the RJ45 hardware console port

> **Warning:** Only **one** console method can be utilized at a time. Connecting a client to one console type will cause the other access methods to behave erratically.

3.1 Connecting to IPMI Web Browser Serial Console

The IPMI interface on the **Netgate 8300** contains a web-based serial console accessible via browser. This client is HTML-based and does not require extra software, only a current web browser.

To access the console:

- Log into the IPMI web interface as described in *Intelligent Platform Management Interface (IPMI)*
- Navigate to **Remote Control > SOL**

3.2 Connecting to IPMI Serial-over-LAN Console

The IPMI Serial-over-LAN (SOL) console can also be accessed via IPMI utilities such as `ipmiconsole` which is included with `freeipmi-tools` via `apt`.

To access the SOL console using `ipmiconsole`:

- Install ipmitool and related utilities from `apt` if they are not already present

  ```
  $ sudo apt update
  $ sudo apt install -y ipmitool freeipmi-tools
  ```

- Run the following command to launch an IPMI SOL session:

  ```
  $ ipmiconsole -h <address> -u <user> -P
  ```

Replace <`address`> with the IP address or hostname of the IPMI interface.

Replace <`user`> with a valid IPMI user with sufficient privileges to access SOL.

The `-P` parameter causes `ipmiconsole` to prompt for a password.

3.3 Connecting to RJ45 Console Port

A separate adapter is required to make a connection between a computer and the firewall using the RJ45 serial port. The **Netgate 8300** device ships with a USB A to RJ45 console cable suitable for this purpose.

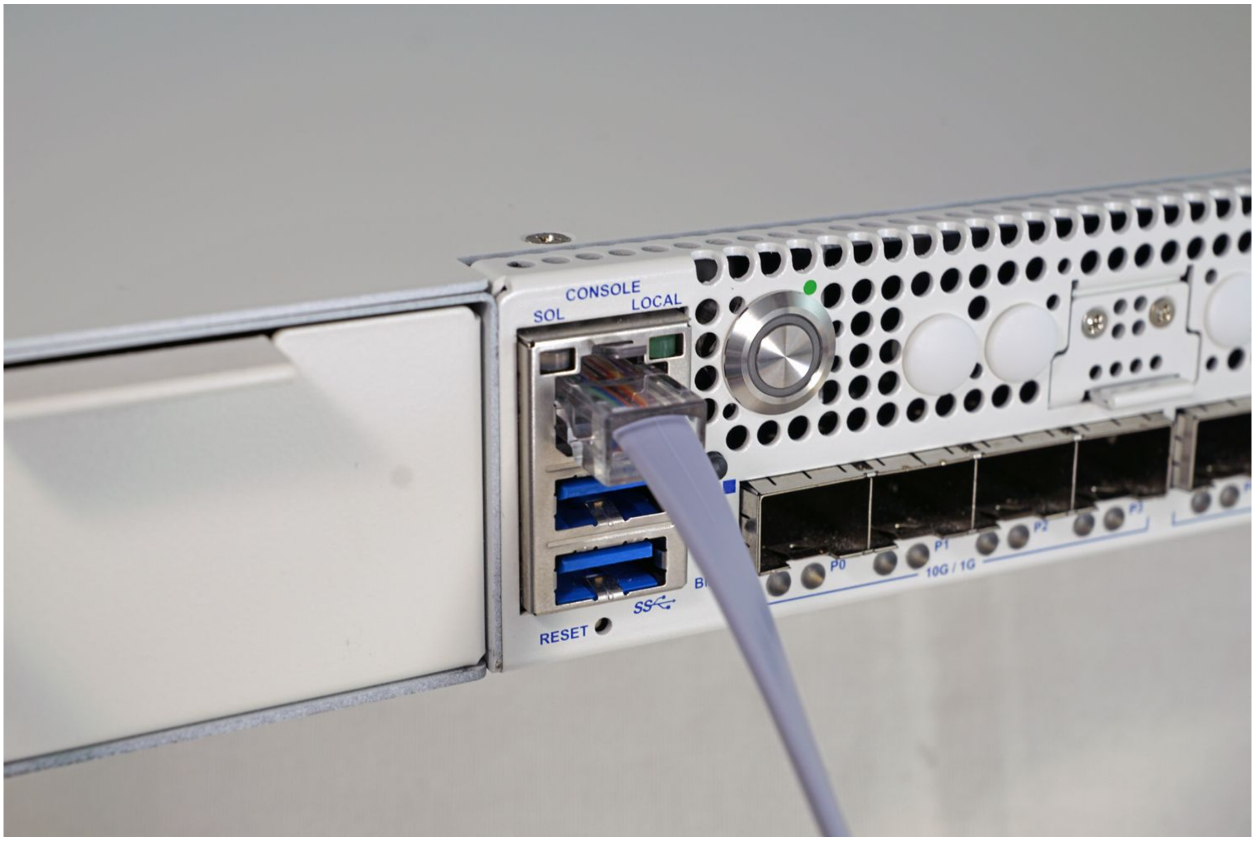


Fig. 1: Serial cable connected to RJ45 Console Port

Any compatible cable may be used instead of the one shipped with the device. This can be a direct **RJ45-to-USB serial** adapter or a standard **USB-to-serial** adapter and an **RJ45-to-DB9** adapter or cable. It is also possible to utilize client hardware serial ports and compatible cables, but these ports are rare on modern hardware.

These are standard components, inexpensive and readily available from most retail outlets that sell computer cables.

Installing drivers and locating the port will vary depending on the third party device, consult its documentation for details.

3.4 Launch a Terminal Program

Use a terminal program to connect to the system console port. Some choices of terminal programs:

Windows

For Windows the best practice is to run *PuTTY in Windows* or SecureCRT. An example of how to configure PuTTY is below.

> **Warning:** Do not use **Hyperterminal**.

macOS

For macOS the best practice is to run GNU `screen`, or `cu`. An example of how to configure GNU `screen` is below.

Linux

For Linux the best practices are to run GNU `screen`, *PuTTY in Linux*, `minicom`, or `dterm`. Examples of how to configure PuTTY and GNU `screen` are below.

FreeBSD

For FreeBSD the best practice is to run GNU `screen` or `cu`. An example of how to configure GNU `screen` is below.

3.4.1 Client-Specific Examples

PuTTY in Windows

- Open PuTTY and select **Session** under **Category** on the left hand side.
- Set the **Connection type** to **Serial**
- Set **Serial line** to the *console port determined previously*
- Set the **Speed** to `115200` bits per second.
- Click the **Open** button

PuTTY will then display the console.

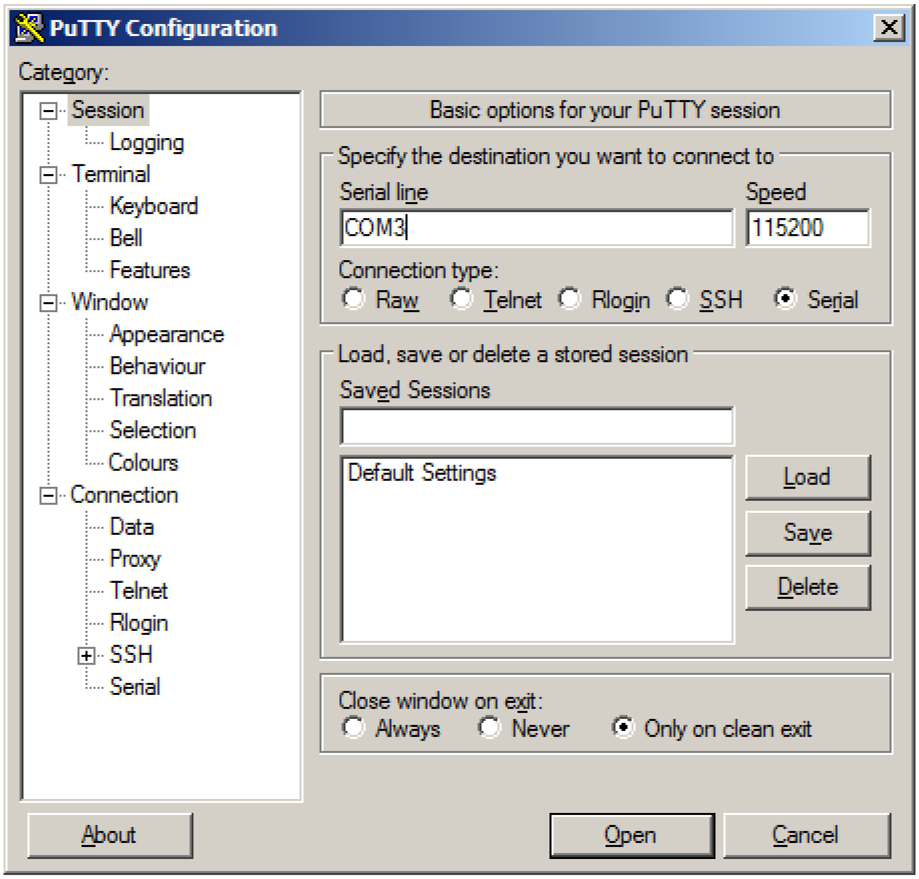
PuTTY in Linux

- Open PuTTY from a terminal by typing `sudo putty`

> **Note:** The `sudo` command will prompt for the local workstation password of the current account.

- Set the **Connection type** to **Serial**
- Set **Serial line** to `/dev/ttyUSB0`
- Set the **Speed** to `115200` bits per second
- Click the **Open** button

PuTTY will then display the console.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM3

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

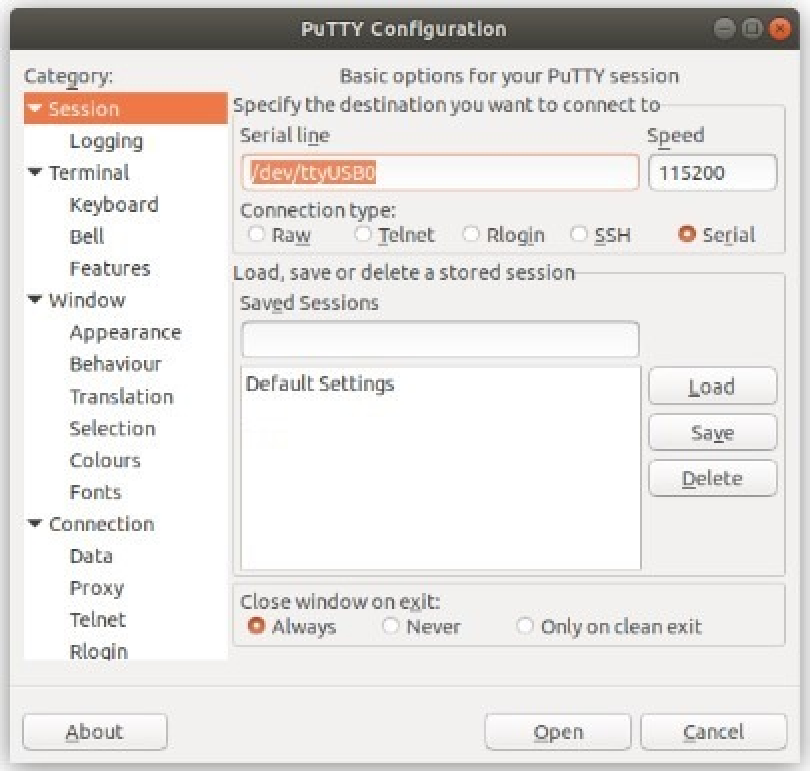
Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Fig. 2: An example of using PuTTY in Windows



Serial line: /dev/ttyUSB0
Speed: 115200
Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial
Close window on exit: ● Always ○ Never ○ Only on clean exit

Fig. 3: An example of using PuTTY in Linux

GNU screen

In many cases `screen` may be invoked simply by using the proper command line, where `<console-port>` is the console port that was located above.

```
$ sudo screen <console-port> 115200
```

Note: The `sudo` command will prompt for the local workstation password of the current account.

If portions of the text are unreadable but appear to be properly formatted, the most likely culprit is a character encoding mismatch in the terminal. Adding the `-U` parameter to the `screen` command line arguments forces it to use UTF-8 for character encoding:

```
$ sudo screen -U <console-port> 115200
```

3.4.2 Terminal Settings

The settings to use within the terminal program are:

Speed
`115200` baud, the speed of the BIOS

Data bits
`8`

Parity
None

Stop bits
`1`

Flow Control
Off or XON/OFF.

> **Warning:** Hardware flow control (RTS/CTS) **must** be disabled.

Terminal Optimization

Beyond the required settings there are additional options in terminal programs which will help input behavior and output rendering to ensure the best experience. These settings vary location and support by client, and may not be available in all clients or terminals.

These are:

Terminal Type
`xterm`

This setting may be under Terminal, Terminal Emulation, or similar areas.

Color Support
ANSI colors / 256 Color / ANSI with 256 Colors

This setting may be under Terminal Emulation, Window Colors, Text, Advanced Terminfo, or similar areas.

Character Set / Character Encoding
`UTF-8`

This setting may be under Terminal Appearance, Window Translation, Advanced International, or similar areas. In GNU screen this is activated by passing the `-U` parameter.

Line Drawing
Look for and enable setting such as "Draw lines graphically", "Use unicode graphics characters", and/or "Use Unicode line drawing code points".

These settings may be under Terminal Appearance, Window Translation, or similar areas.

Function Keys / Keypad
`Xterm R6`

In Putty this is under **Terminal > Keyboard** and is labeled **The Function Keys and Keypad**.

Font
For the best experience, use a modern monospace unicode font such as Deja Vu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.

This setting may be under Terminal Appearance, Window Appearance, Text, or similar areas.

3.5 What's Next?

After connecting a terminal client, it may not immediately see any output. This could be because the device has already finished booting or it may be that the device is waiting for some other input.

If the device does not yet have power applied, plug it in and monitor the terminal output.

If the device is already powered on, try pressing `Space`. If there is still no output, press `Enter`. If the device was booted, it should redisplay the login prompt or produce other output indicating its status.

3.6 Troubleshooting

3.6.1 Serial Device Missing

With a USB serial console there are a few reasons why the serial port may not be present in the client operating system, including:

No Power

Some models require power before the client can connect to the USB serial console.

USB Cable Not Plugged In

For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.

Bad USB Cable

Some USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.

The ideal cable to use is the one that came with the device. Failing that, ensure the cable is of the correct type and specifications, and try multiple cables.

Wrong Device

In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.

Hardware Failure

There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

3.6.2 No Serial Output

If there is no output at all, check the following items:

USB Cable Not Plugged In

For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.

Wrong Device

In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.

Wrong Terminal Settings

Ensure the terminal program is configured for the correct speed. The default BIOS speed is `115200`, and many other modern operating systems use that speed as well.

Some older operating systems or custom configurations may use slower speeds such as `9600` or `38400`.

Device OS Serial Console Settings

Ensure the operating system is configured for the proper console (e.g. `ttyS1` in Linux). Consult the various operating install guides on this site for further information.

3.6.3 PuTTY has issues with line drawing

PuTTY generally handles most cases OK but can have issues with line drawing characters on certain platforms.

These settings seem to work best (tested on Windows):

Window

Columns x Rows

`80x24`

Window > Appearance

Font

Courier New 10pt or *Consolas 10pt*

Window > Translation

Remote Character Set

Use font encoding or *UTF-8*

Handling of line drawing characters

Use font in both ANSI and OEM modes or *Use Unicode line drawing code points*

Window > Colours

Indicate bolded text by changing

The colour

3.6.4 Garbled Serial Output

If the serial output appears to be garbled, missing characters, binary, or random characters check the following items:

Flow Control

In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.

On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the **Flow Control** option is in the settings tree under **Connection**, then **Serial**.

To disable flow control in GNU Screen, add the `-ixon` and/or `-ixoff` parameters after the serial speed as in the following example:

```
$ sudo screen <console port> 115200,-ixon
```

Terminal Speed

Ensure the terminal program is configured for the correct speed. (See *No Serial Output*)

Character Encoding

Ensure the terminal program is configured for the proper character encoding, such as **UTF-8** or **Latin-1**, depending on the operating system. (See *GNU Screen*)

3.6.5 Serial Output Stops After the BIOS

If serial output is shown for the BIOS but stops afterward, check the following items:

Terminal Speed

Ensure the terminal program is configured for the correct speed for the installed operating system. (See *No Serial Output*)

Device OS Serial Console Settings

Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. `ttyS1` in Linux). Consult the various operating install guides on this site for further information.

Bootable Media

If booting from a USB flash drive, ensure that the drive was written correctly and contains a bootable operating system image.

CHAPTER

FOUR

INTELLIGENT PLATFORM MANAGEMENT INTERFACE (IPMI)

The **Netgate 8300** appliance includes a baseboard management controller (BMC) for out-of-band (OOB) access via Intelligent Platform Management Interface (IPMI). Administrators can use this interface to control the hardware itself, such as power on/off, access a serial over LAN (SOL) console, mount virtual media for installation, see hardware status events, and more.

IPMI Usage Topics

4.1 Accessing IPMI

To access IPMI via its web-based GUI, navigate to the IP address of the BMC using a web browser, e.g. `https://10.10.10.89`. It can also be accessed using ipmitool over the network.

By default, the dedicated IPMI network port (**P11**) is configured to be a DHCP client but it can be manually configured with a static address.

The address of the BMC set to DHCP can be determined in a few different ways:

- Enter the BIOS when powering on the device and navigate to **Server Mgmt > BMC Network Configuration**. That screen displays the current network information for the BMC.
- From the installed Operating System, run `ipmitool lan print 2` to output the current BMC/IPMI network configuration for the dedicated IPMI network port.
- Check the DHCP server leases to see which lease was allocated to the BMC.

Tip: The MAC address of the BMC is printed on the device label for reference.

4.2 Default IPMI Credentials

The default IPMI username is `root` and the default password is `root`.

In compliance with privacy legislation, the Username and Password to access the IPMI port on the **Netgate 8300 must be changed** on first access.

The IPMI web interface will present a screen to change the password immediately upon the first login using the default credentials.

To change the password:

- Navigate to the IPMI address using a web browser
- Log in to the IPMI Web Console with the default credentials.
- Enter the following items on the **Change Password** form:

  Old Password
  The current default password (`root`).

  New Password
  The new password to set. If the password is acceptable, the field will be outlined in green. If the password is invalid, the field will be outlined in red.

  See also:

  For a list of password requirements, see the next section. The IPMI Web Console will also print the requirements if a user attempts to set a password it considers too weak.

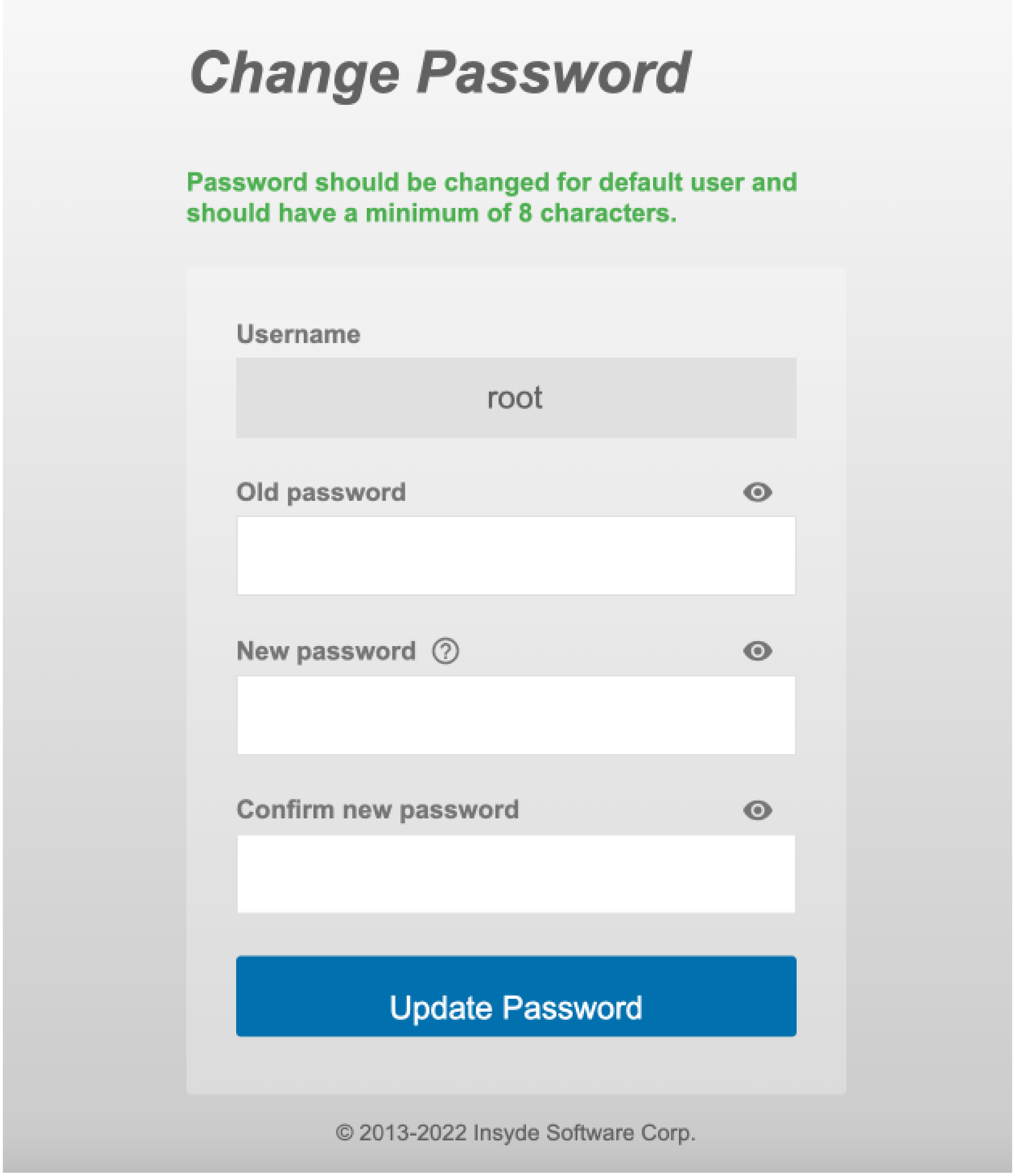
  Confirm Password
  The same password as in the **New Password** field. If the passwords match, the field will be outlined in green. If the passwords do not match, the field will be outlined in red.

- Click **Update Password**

4.3 IPMI Password Requirements

IPMI user account passwords must meet the following criteria:

- Minimum of 6 characters long
- Contains only printable ASCII characters
- Cannot contain the account name (Case insensitive)
- Meets at least 3 of following criteria:
  - Contains uppercase characters (`A` through `Z`)
  - Contains lowercase characters (`a` through `z`)
  - Contains numbers (`0` through `9`)
  - Contains special characters (e.g., `$`, `&`)



Change Password

Password should be changed for default user and should have a minimum of 8 characters.

Username

root

Old password

New password ?

Confirm new password

Update Password

© 2013-2022 Insyde Software Corp.

Fig. 1: IPMI Web Console forcing a password change on first login

4.4 Changing the IPMI Password

The IPMI password for **Netgate 8300** appliances can be changed either through the browser-based IPMI console or by using the ipmitool utility.

4.4.1 Using IPMI Web Console

To change the IPMI password in the web console:

- Navigate to the IPMI address using a web browser
- Log in to the IPMI console with the current credentials

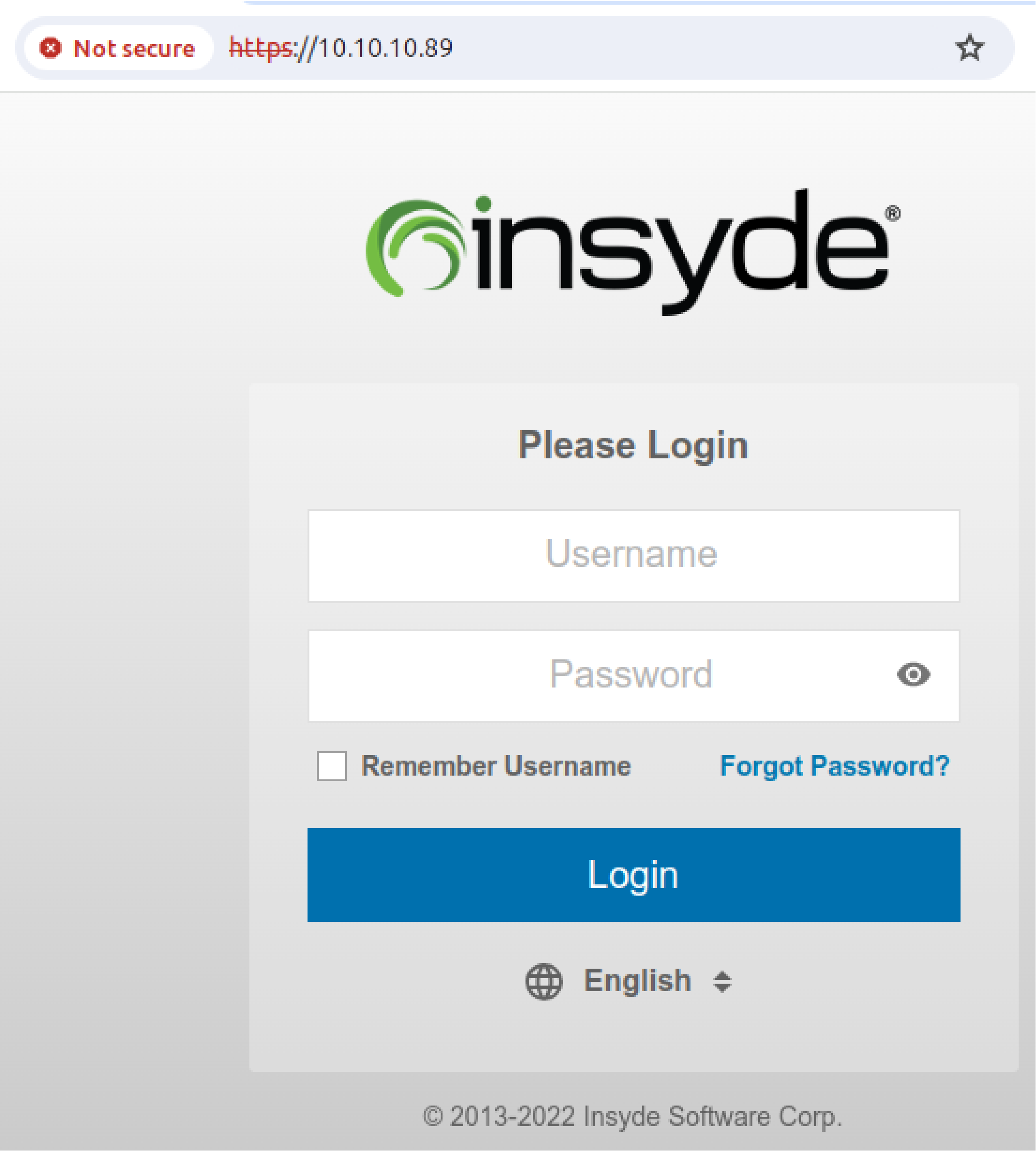


Fig. 2: Log Into IPMI

Note: If the username is not known, see the next section for information on how to use `ipmitool` to view the current user list.

- Navigate to **Configuration > Users**

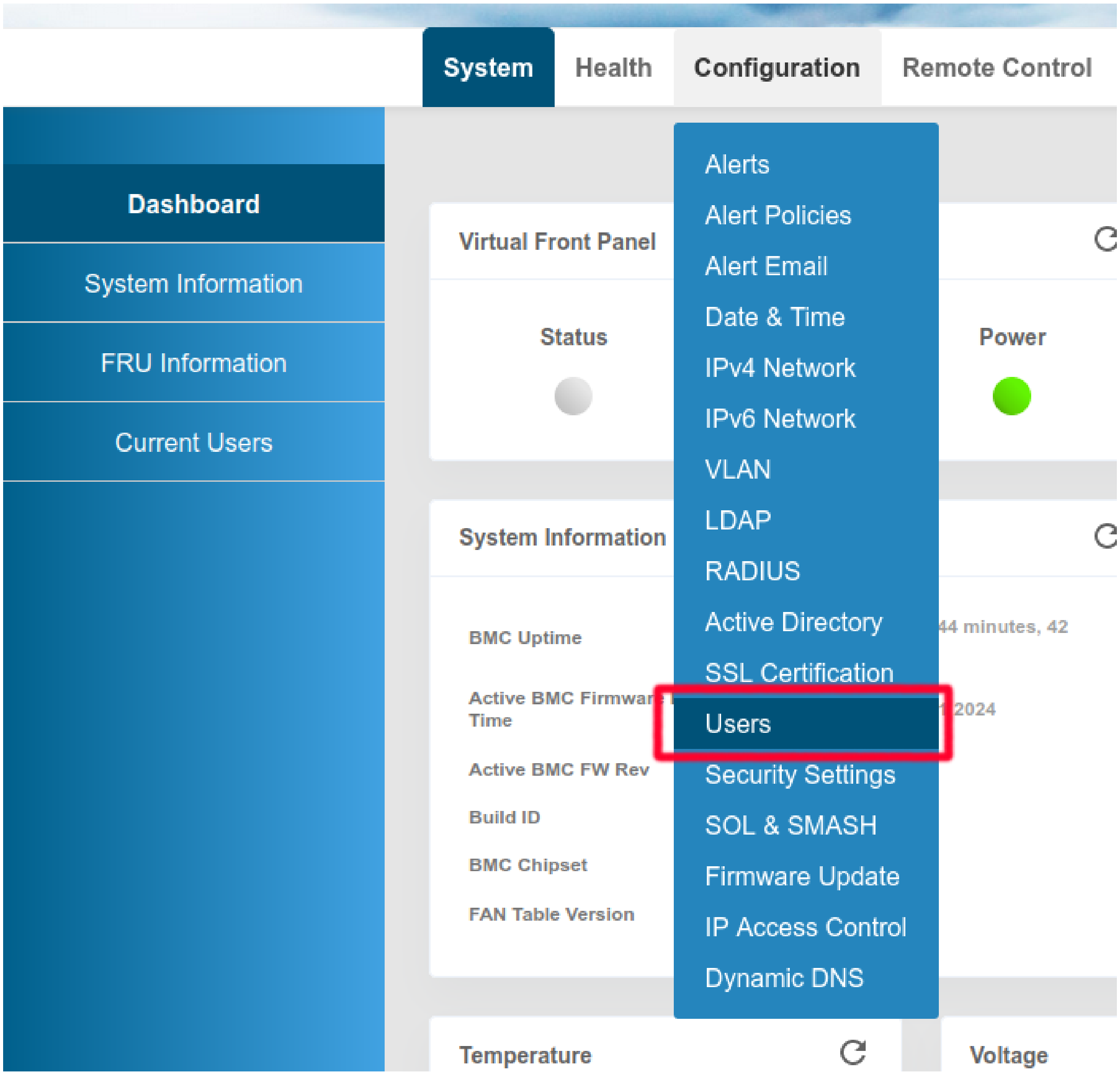
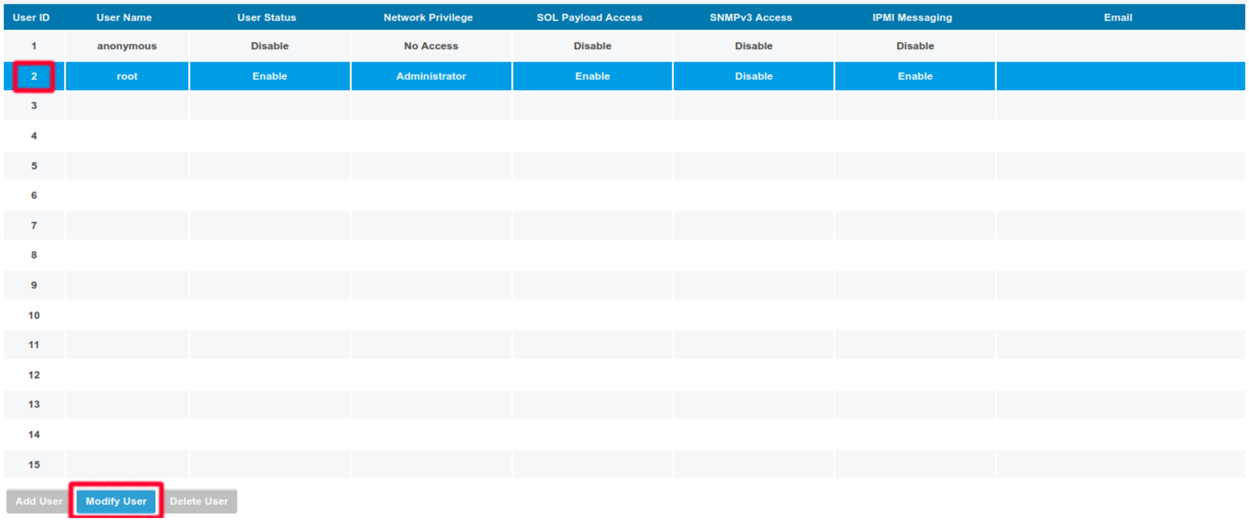


Fig. 3: Configuration > Users

- Select the user to modify by clicking on its row in the list

  This is likely the `root` user or another user with *Administrator* privileges, typically the user in the second slot (User ID **2**).

- Click **Modify User**
- Set the form fields as follows:



User ID	User Name	User Status	Network Privilege	SOL Payload Access	SNMPv3 Access	IPMI Messaging	Email
1	anonymous	Disable	No Access	Disable	Disable	Disable	
2	root	Enable	Administrator	Enable	Disable	Enable	
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Fig. 4: Modify User

User Name
Change the username from the default `root` to a personalized name

This is optional, but a best practice.

Change Password
Click to enable the slider

Password
Enter the new **Password**

If the password is acceptable, the field will be outlined in green. If the password is invalid, the field will be outlined in red.

See also:

For a list of password requirements, see the previous section.

Confirm Password
Enter the new password again in **Confirm Password**

If the passwords match, the field will be outlined in green. If the passwords do not match, the field will be outlined in red.

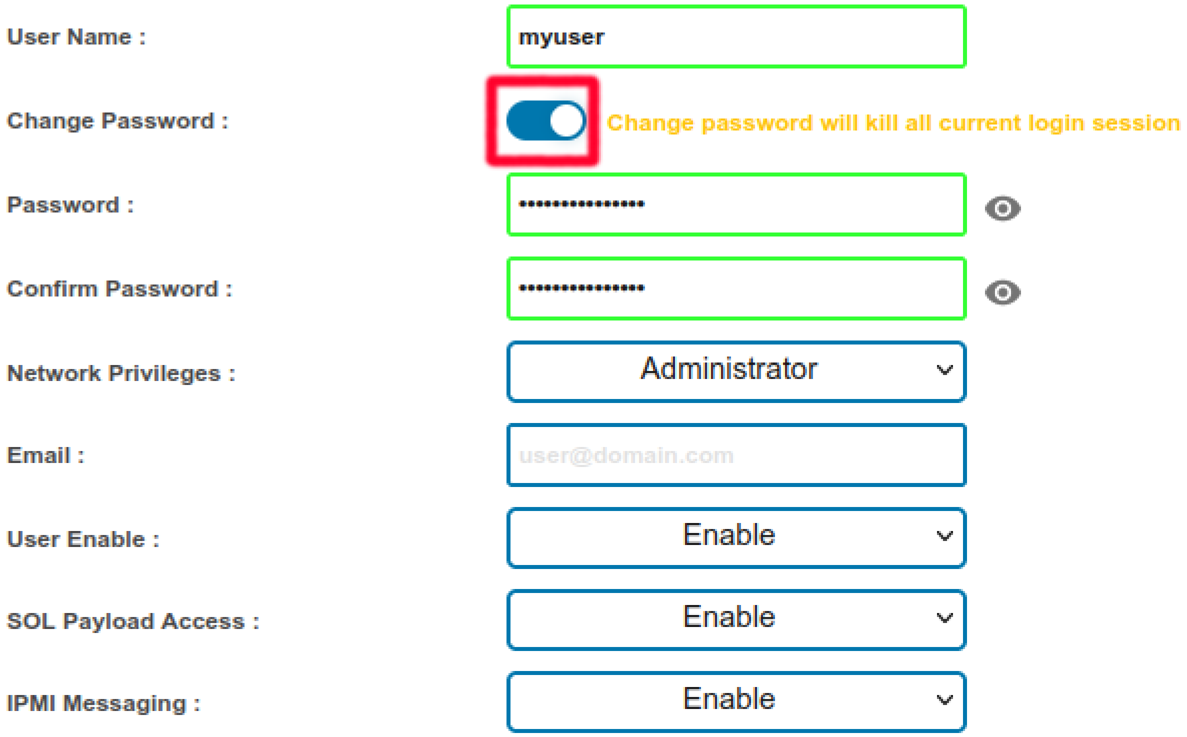
- Click **Modify**
- Click **Confirm** on the alert that says “Modified user successfully.”

4.4.2 Using the ipmitool Utility

If the IPMI web interface is unavailable or the current password is unknown, the `ipmitool` utility available via `apt` can change the password.

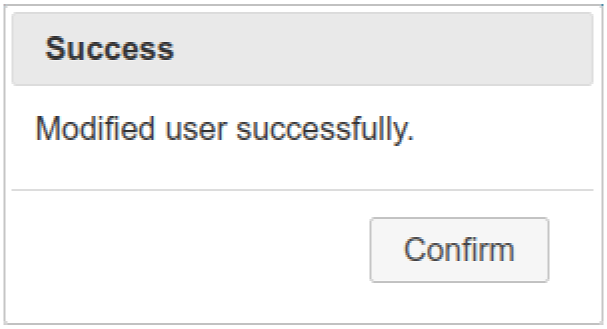
These commands may be performed from the TNSR CLI (`host shell sudo <command>`) or a shell prompt (`sudo <command>`).

The following steps assumine the procedure is being performed locally on the **Netgate 8300** from a shell prompt.



User Name :	myuser
Change Password :	● Change password will kill all current login session
Password :	••••••••••••••••
Confirm Password :	••••••••••••••••
Network Privileges :	Administrator
Email :	user@domain.com
User Enable :	Enable
SOL Payload Access :	Enable
IPMI Messaging :	Enable

Fig. 5: Modify User Form



Success

Modified user successfully.

Fig. 6: Click Confirm

Note: To reach a shell prompt in TNSR, use the `host shell` command.

- Install ipmitool and related utilities from `apt` if they are not already present

  ```
  $ sudo apt update
  $ sudo apt install -y ipmitool freeipmi-tools
  ```

- List the current IPMI users

  ```
  $ sudo ipmitool user list
  ```

  Note: **Netgate 8300** appliances use the user name `root` by default.

  The command prints a list of users, for example:

  ```
  ID  Name             Callin  Link Auth  IPMI Msg   Channel Priv Limit
  1                    true    false      false      NO ACCESS
  2   root             true    false      true       ADMINISTRATOR
  3                    true    false      false      NO ACCESS
  4                    true    false      false      NO ACCESS
  5                    true    false      false      NO ACCESS
  6                    true    false      false      NO ACCESS
  7                    true    false      false      NO ACCESS
  8                    true    false      false      NO ACCESS
  9                    true    false      false      NO ACCESS
  10                   true    false      false      NO ACCESS
  11                   true    false      false      NO ACCESS
  12                   true    false      false      NO ACCESS
  13                   true    false      false      NO ACCESS
  14                   true    false      false      NO ACCESS
  15                   true    false      false      NO ACCESS
  ```

  Warning: Usernames are case-sensitive.

- Reset the password for a user

  The default `root` user is User ID `2`, and the example below sets the password for this user to `NETGATE`.

  ```
  $ sudo ipmitool user set password 2 NETGATE
  ```

  Warning: This password is for example purposes only. Use a secure password.

  If successful, the output will be:

  ```
  Set User Password command successful (user 2)
  ```

4.5 Reset IPMI Network Configuration

The `ipmitool` utility can also change or reset the network configuration of the IPMI interface if it cannot be reached over the network.

These commands may be performed from the TNSR CLI (`host shell sudo <command>`) or a shell prompt (`sudo <command>`).

The following steps assumine the procedure is being performed locally on the **Netgate 8300** from a shell prompt.

Note: To reach a shell prompt in TNSR, use the `host shell` command.

Note: The dedicated IPMI port (**P11**) is on IPMI network channel **2**.

- Install ipmitool and related utilities from `apt` if they are not already present

  ```
  $ sudo apt update
  $ sudo apt install -y ipmitool freeipmi-tools
  ```

- Set the IPMI IP address and subnet mask

  The following commands configure the IP address of the IPMI interface and its corresponding subnet mask in dotted quad notation.

  This example sets the IPMI IP address to `172.31.123.5/24`:

  ```
  $ sudo ipmitool lan set 2 ipaddr 172.31.123.5
  $ sudo ipmitool lan set 2 netmask 255.255.255.0
  ```

- Set the IPMI gateway IP address

  To communicate with IPMI outside of its configured subnet, the IPMI interface must have a default gateway set.

  This example sets the default gateway to `172.31.123.1`.

  ```
  $ sudo ipmitool lan set 2 defgw ipaddr 172.31.123.1
  ```

- Enable IPMI access on the interface

  ```
  $ sudo ipmitool lan set 2 access on
  ```

4.6 Re-arm the Chassis Intrusion Switch

The chassis on **Netgate 8300** has an intrusion detection function which can be reset via IPMI. See *Re-arm the Chassis Intrusion Switch* for details.

CHAPTER

FIVE

UPDATING THE BASEBOARD MANAGEMENT CONTROLLER FIRMWARE

Occasionally there are updates to the Baseboard Management Controller (BMC) firmware on the **Netgate 8300** to address problems or improve features. This firmware can be updated using the web interface on the BMC which also contains Intelligent Platform Management Interface (IPMI) functionality.

5.1 Warnings & Precautions

Warning: The firmware should only be updated at the direction of Netgate TAC.

Warning: The device must be rebooted multiple times during this process. This reboots the BMC and the operating system, which will disrupt traffic passing through the device.

Warning: Completing this process requires removing power to the device temporarily, which requires physical access or separate out of band power control.

Warning: As a part of this update process the BMC must be factory reset, which will remove any customizations made to the BMC and IPMI, including any network configuration, additional users, and any password changes.

5.2 Obtain the Firmware Update File

Before starting, contact Netgate TAC and request the BMC firmware update file. It will have a filename such as `BMC_FW-Update.bin` and may be compressed. If it is compressed, decompress it before proceeding.

The file should be on the same computer with the web browser being used to access the BMC web interface.

5.3 Connect to the Web Interface

This update is performed in the browser-based web interface on the BMC. To access this web interface, follow the directions in *Intelligent Platform Management Interface (IPMI)*.

Tip: As this update process requires a factory reset, make sure to note any customized settings before proceeding so they can be reconfigured after the update is complete.

5.4 Update the Firmware

- Navigate to **Configuration > Firmware Update** in the web interface.

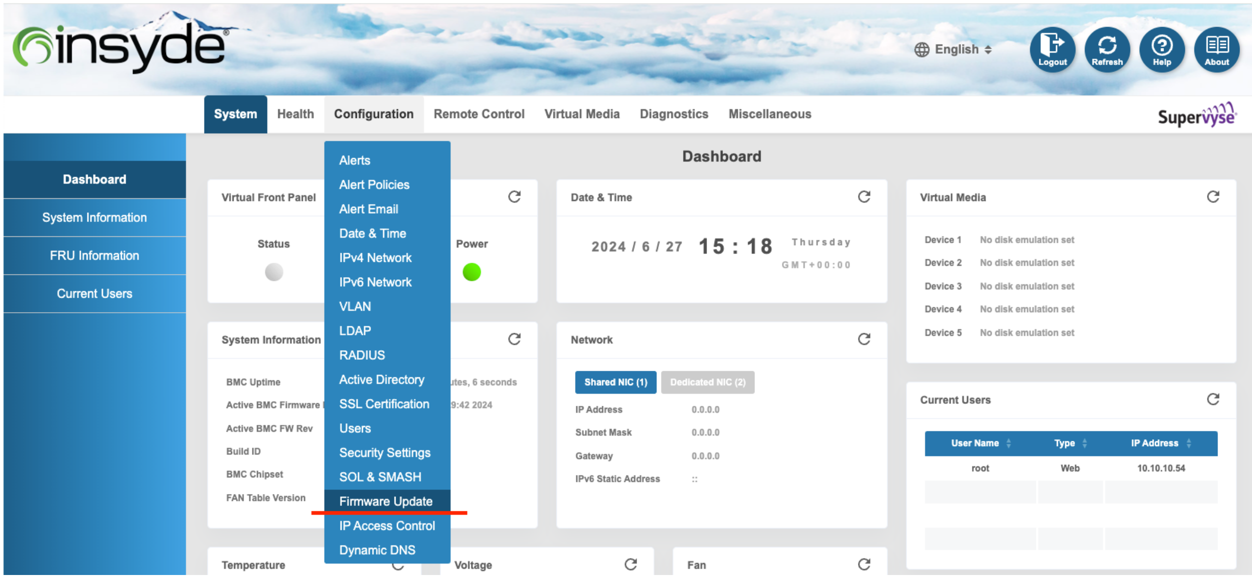
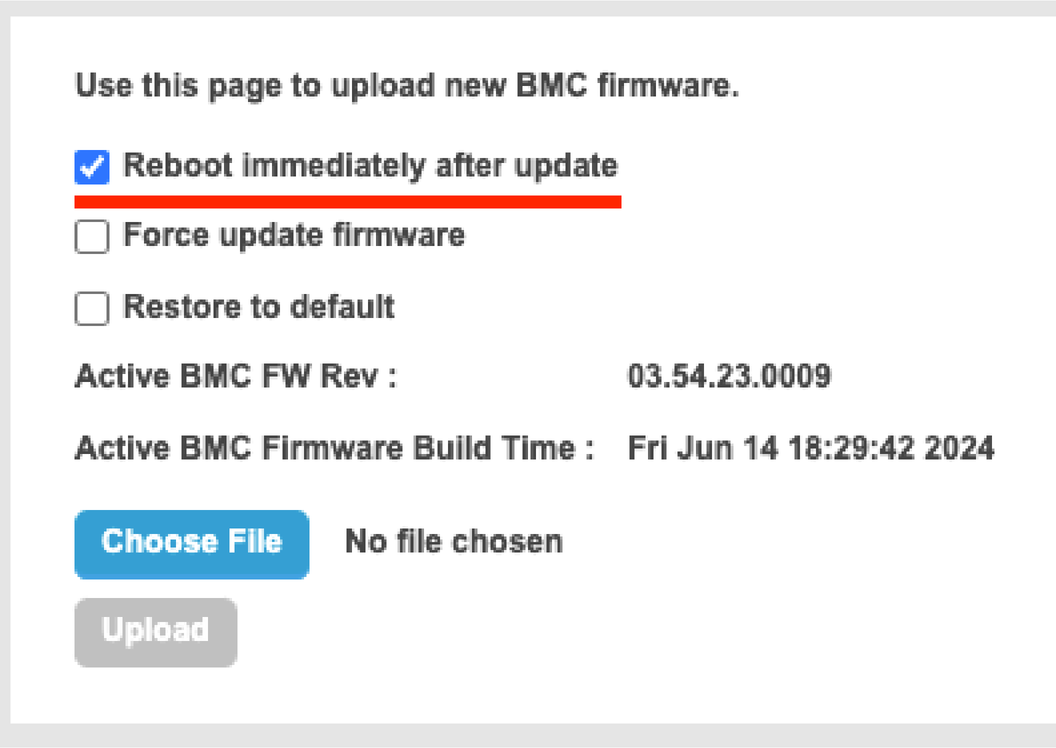


Fig. 1: Firmware Update menu location

- Check **Reboot immediately after update**.

> **Warning:** This reboots the BMC **and** the operating system.

- Click **Choose File**
- Select the firmware update file (e.g. `BMC_FW-Update.bin`).
- Click **Upload** to start the upload process.
- Wait until the upload process is 100% complete.
- Click **Update** to start the BMC firmware update process.
- Wait for the update to complete and for the device to reboot.
- Log back into the BMC web interface.
- Verify the BMC version.



Use this page to upload new BMC firmware.

☑ Reboot immediately after update

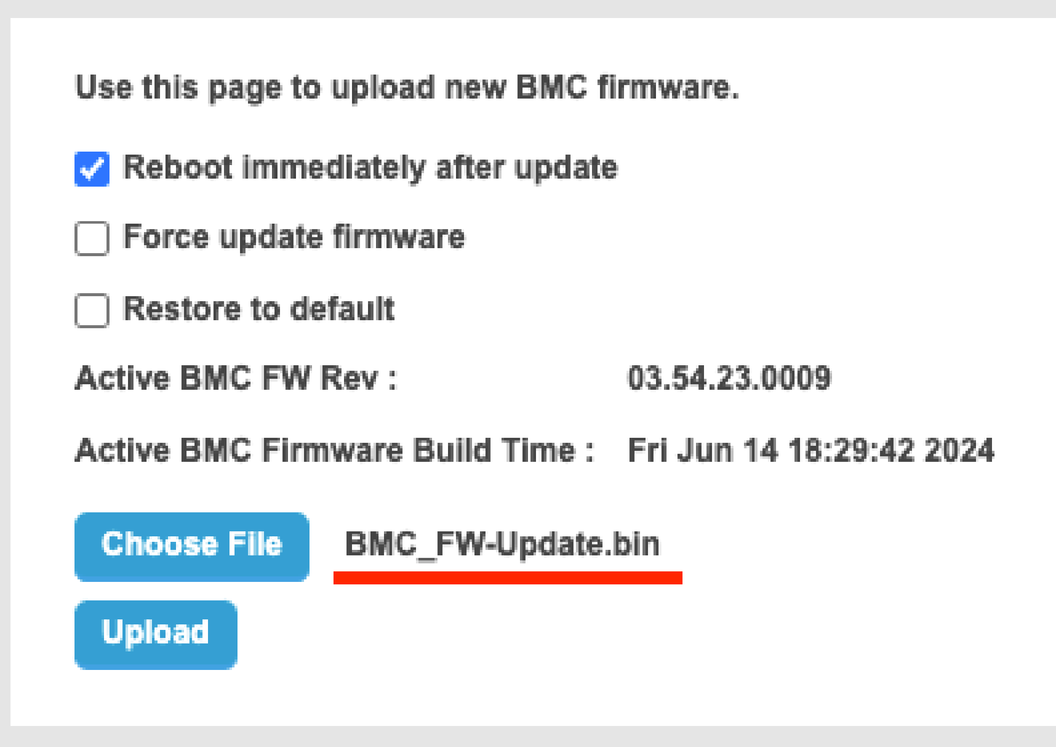
□ Force update firmware

□ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Fig. 2: Check the box to automatically reboot when the update finishes



Use this page to upload new BMC firmware.

☑ Reboot immediately after update

□ Force update firmware

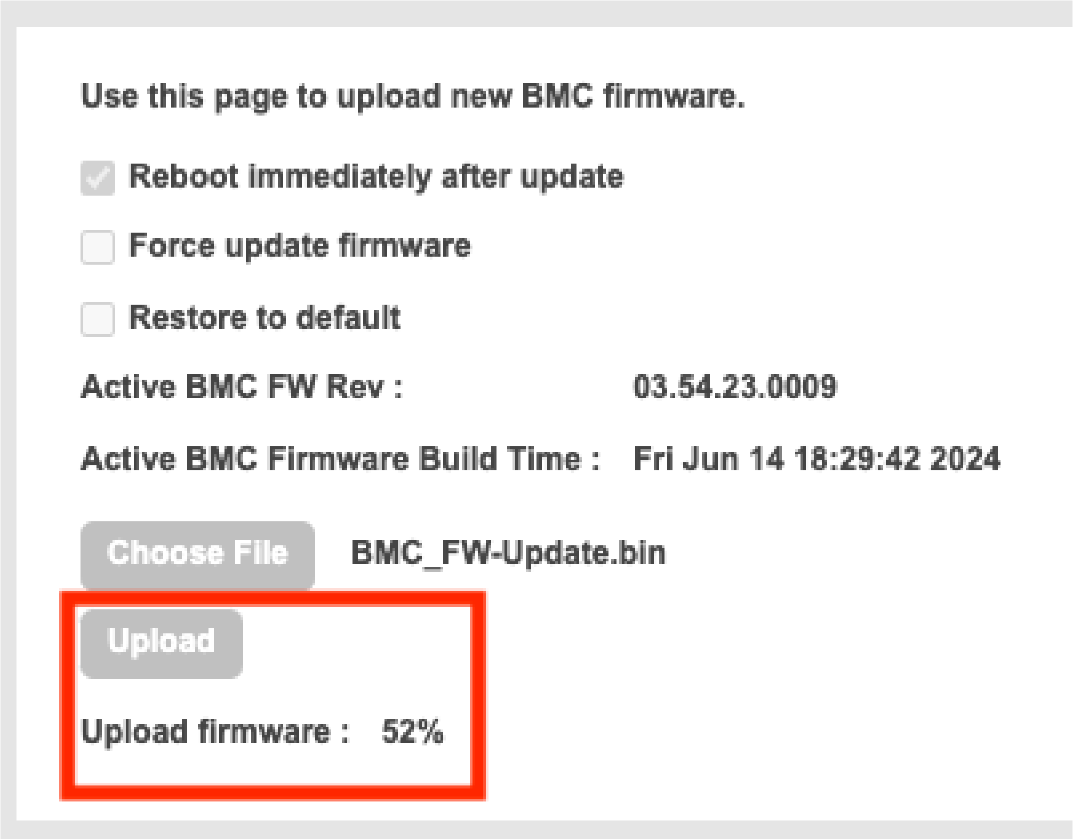
□ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

BMC_FW-Update.bin

Fig. 3: Select the firmware update file (e.g. `BMC_FW-Update.bin`)



Use this page to upload new BMC firmware.

☑ Reboot immediately after update

□ Force update firmware

□ Restore to default

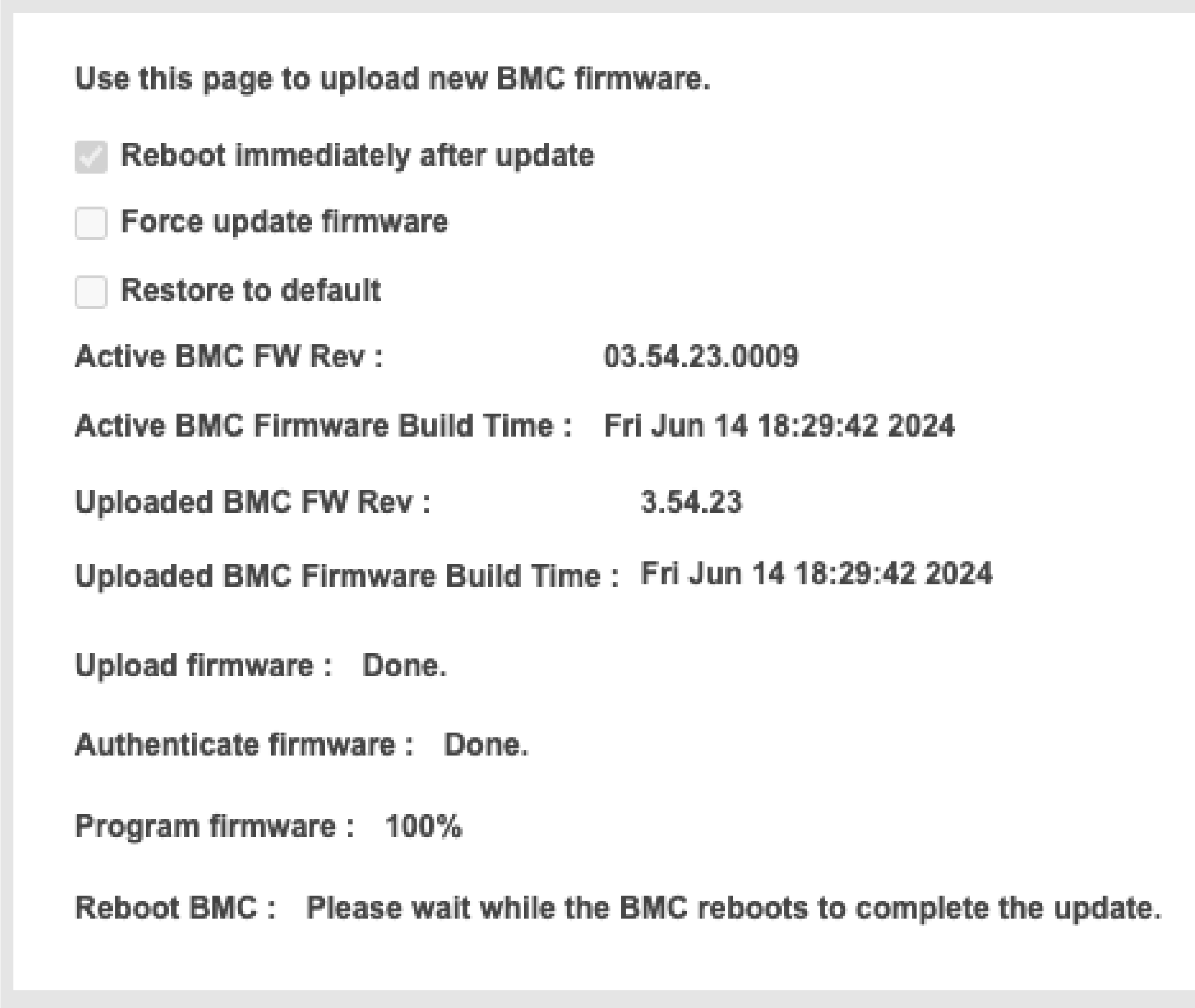
Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

BMC_FW-Update.bin

Upload firmware : 52%

Fig. 4: Firmware file upload in progress



Use this page to upload new BMC firmware.

☑ Reboot immediately after update

□ Force update firmware

□ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Uploaded BMC FW Rev : 3.54.23

Uploaded BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

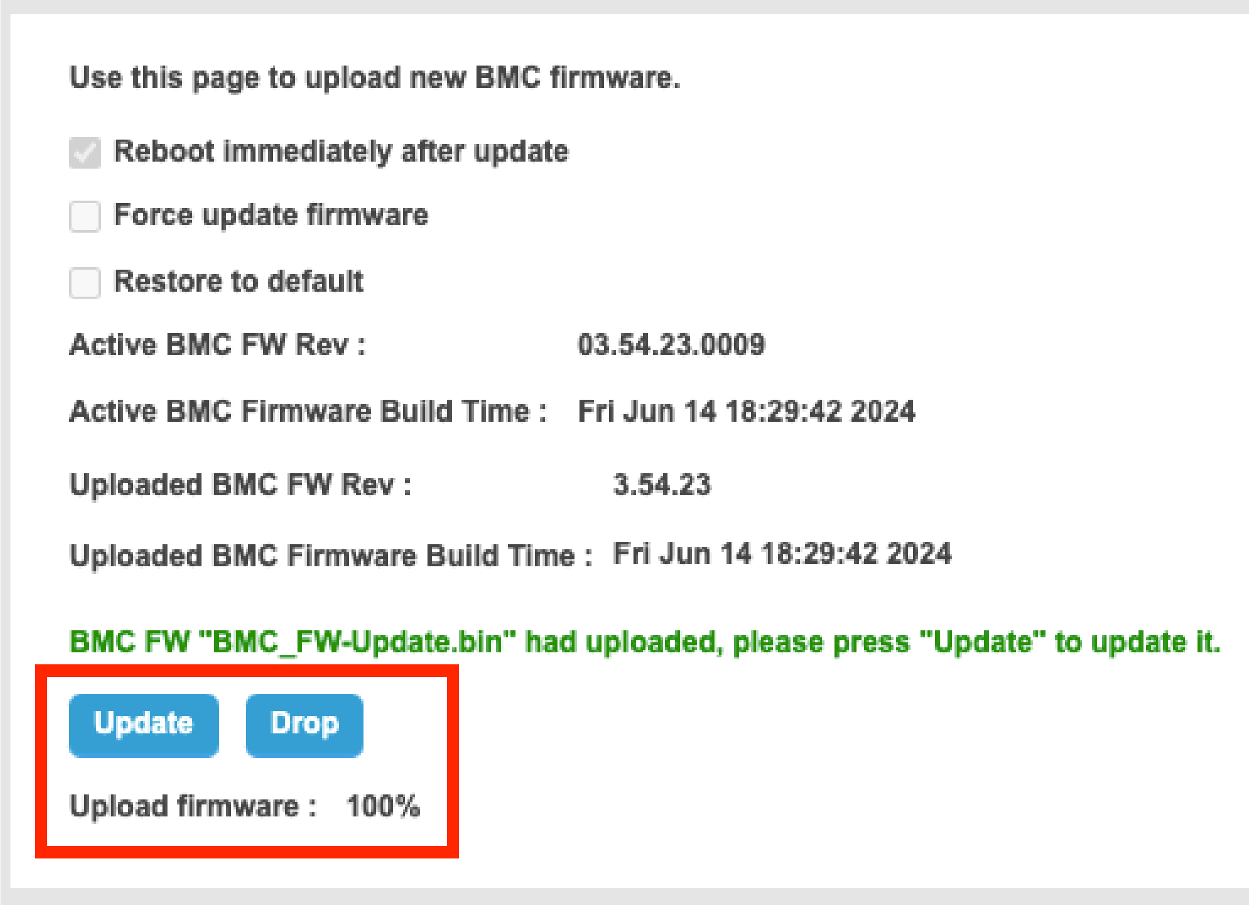
Upload firmware : Done.

Authenticate firmware : Done.

Program firmware : 100%

Reboot BMC : Please wait while the BMC reboots to complete the update.

Fig. 5: Firmware update in progress



Use this page to upload new BMC firmware.

☑ Reboot immediately after update

□ Force update firmware

□ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

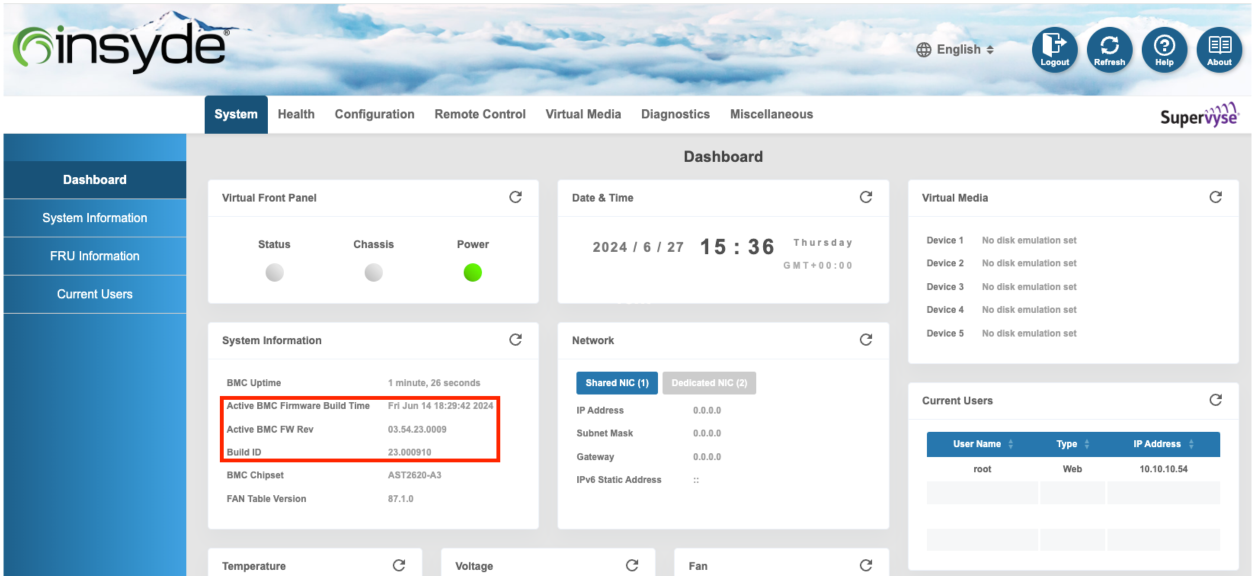
Uploaded BMC FW Rev : 3.54.23

Uploaded BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

BMC FW "BMC_FW-Update.bin" had uploaded, please press "Update" to update it.

Upload firmware : 100%

Fig. 6: Click **Update** to perform the firmware update



Dashboard

Virtual Front Panel

Status	Chassis	Power
●	●	●

Date & Time

2024 / 6 / 27 15 : 36 Thursday GMT+00:00

Virtual Media

Device 1	No disk emulation set
Device 2	No disk emulation set
Device 3	No disk emulation set
Device 4	No disk emulation set
Device 5	No disk emulation set

System Information

BMC Uptime	1 minute, 26 seconds
Active BMC Firmware Build Time	Fri Jun 14 18:29:42 2024
Active BMC FW Rev	03.54.23.0009
Build ID	23.000910
BMC Chipset	AST2620-A3
FAN Table Version	87.1.0

Network

Shared NIC (1) Dedicated NIC (2)

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
IPv6 Static Address	::

Current Users

User Name	Type	IP Address
root	Web	10.10.10.54

Temperature

Voltage

Fan

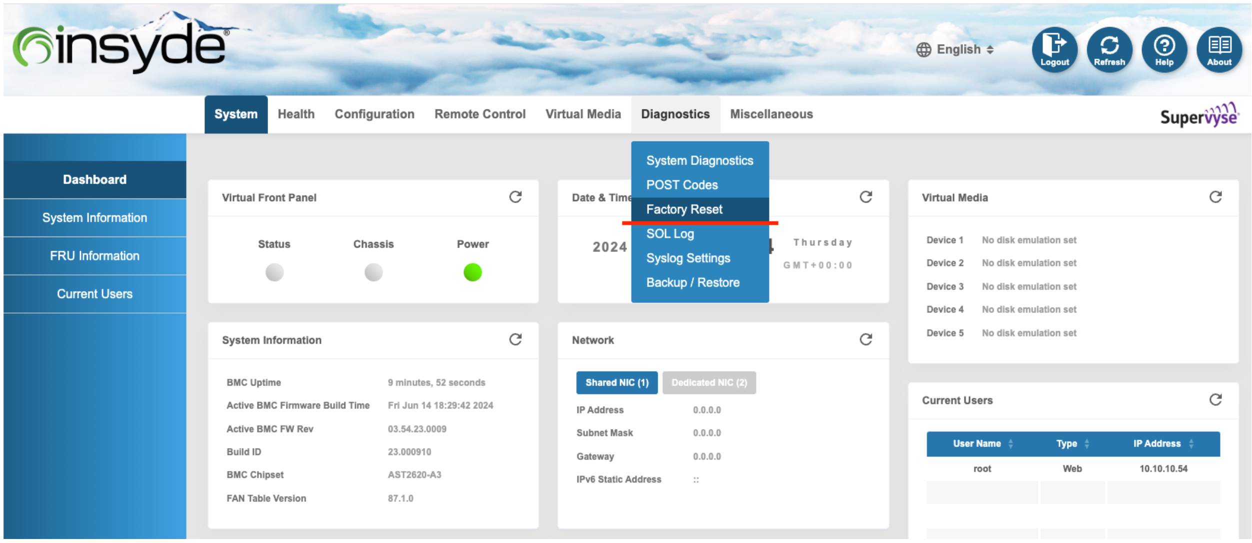
Fig. 7: Checking the BMC firmware version

5.5 Factory Reset

To complete the update, the BMC must be factory reset.

> **Warning:** This factory reset will remove any custom settings, including network configurations, additional users, and password changes.

- Navigate to **Diagnostics > Factory Reset**.



System Information

BMC Uptime 9 minutes, 52 seconds
Active BMC Firmware Build Time Fri Jun 14 18:29:42 2024
Active BMC FW Rev 03.54.23.0009
Build ID 23.000910
BMC Chipset AST2620-A3
FAN Table Version 87.1.0

Network

IP Address 0.0.0.0
Subnet Mask 0.0.0.0
Gateway 0.0.0.0
IPv6 Static Address ::

Virtual Media

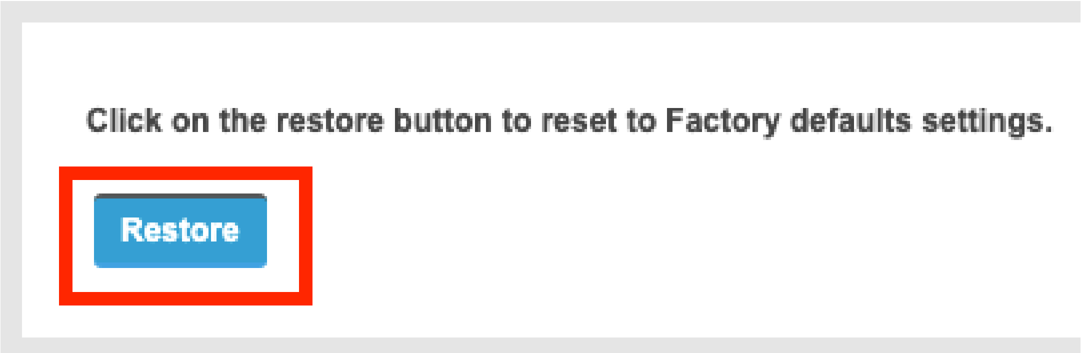
Device 1 No disk emulation set
Device 2 No disk emulation set
Device 3 No disk emulation set
Device 4 No disk emulation set
Device 5 No disk emulation set

Current Users

User Name	Type	IP Address
root	Web	10.10.10.54

Fig. 8: Factory Reset menu location

- Click **Restore** to start the factory reset process.



Click on the restore button to reset to Factory defaults settings.

Fig. 9: Click **Restore** to perform the factory reset

- Shut down and turn off power to the device.

> **Note:** To fully power off the device, switch off or unplug **all** power supplies.

- Restore power to the device.
- Wait for the device to boot.

- Log back into the BMC web interface with the default credentials and change the password.

Tip: When logging back in after the factory reset, use the default credentials and change the password as described in *Intelligent Platform Management Interface (IPMI)*.

- Change any other settings and make any other customizations as needed.

CHAPTER

SIX

RE-ARM THE CHASSIS INTRUSION SWITCH

The chassis on **Netgate 8300** has an intrusion detection function. If the chassis has been opened the intrusion switch will be tripped even if the power was off.

Note: Chassis intrusion switch events and the current status of the sensor can be viewed in the IPMI web interface (*Intelligent Platform Management Interface (IPMI)*), but the only supported method to re-arm the sensor at this time is via IPMI CLI utilities.

Warning: While the intrusion alarm is active the system fans run at a higher fixed speed than normal. Re-arming the intrusion sensor returns the fan to their typical profiled speeds.

6.1 Re-arm Using IPMI CLI Utilities

The intrusion switch can be re-armed using ipmitool either locally or over the network.

These commands may be performed from the TNSR CLI (`host shell sudo <command>`) or a shell prompt (`sudo <command>`).

The following steps assumine the procedure is being performed locally on the **Netgate 8300** from a shell prompt.

Note: To reach a shell prompt in TNSR, use the `host shell` command.

- Replace and fasten the chassis cover completely.
- Install ipmitool and related utilities from `apt` if they are not already present

```
$ sudo apt update
$ sudo apt install -y ipmitool freeipmi-tools
```

- Re-arm chassis intrusion sensor two times:

```
$ sudo ipmitool raw 0x04 0x2a 0x04 0x00
$ sudo ipmitool raw 0x04 0x2a 0x04 0x00
```

- Check the Chassis intrusion sensor, it should read a value of `0x0080`

```
$ sudo ipmitool sensor list | grep -i physical
Physical Scrty | 0x0 | discrete | 0x0080| na | na | na | na | na | na
```

CHAPTER

SEVEN

M.2 NVME SSD INSTALLATION

The Netgate® 8300 ships with one PCIe-based M.2 NVMe SSD. Optionally, a second PCIe-based M.2 NVMe drive can be installed as an upgrade.

Note: This guide assumes a second disk is being added for redundancy via software RAID disk mirroring.

M.2 NVMe SSD Installation Outline

7.1 Warnings and Precautions

Danger: Anti-static protection must be used throughout this procedure.

Warning: TNSR® software must be reinstalled using a software RAID mirror configuration to use a second M.2 NVMe SSD for redundancy.

Warning: The Netgate 8300 only supports PCIe-based M.2 NVMe storage devices. It **does not** support M.2 SATA devices.

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and M.2 cards. There are many delicate components which can be damaged during this process. **Damage caused via physical contact and electrostatic discharge while performing this installation is not covered by the warranty**.

> **Warning:** This device includes an intrusion detection sensor which operates even when the device is without power.
>
> Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in *Re-arm the Chassis Intrusion Switch*.
>
> When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

7.2 Required Tools and Hardware

Installing an M.2 NVMe SSD in the Netgate 8300 requires the following tools and hardware:

- Phillips screwdriver
- Anti-static grounding strap and anti-static mat for handling bare M.2 card and 8300 system
- 1 x PCIe-based M.2 NVMe SSD, 2280 or 2242 size, B+M-key or M-key card

See also:

The M.2 slot accepts both 2280 and 2242 size cards, but the device ships with the retaining clip set for a 2280 size card by default. This clip can easily be moved to accommodate a 2242 card without any tools.

7.3 Installation Procedure

The installation procedure has many steps which are broken down into related groups in the remainder of this document. Follow all steps in the procedure carefully.

7.3.1 Take a Backup

If the system contains an existing configuration, then the first step is to take a backup of that configuration for safety.

If the existing configuration is not necessary, this section may be skipped.

There are numerous backup options covered in the TNSR software documentation section on Backup and Restore.

7.3.2 Download the Installer

Before proceeding further, download a copy of the TNSR installer using a Netgate Store Account and write the installer to a USB memstick.

7.3.3 Power Off and Disconnect

Installing the SSD requires removing the top of the case to expose the internal components. For safety, before opening the case, the Netgate 8300 must be **completely** disconnected from everything. This includes power, network cables, USB cables, serial console cables, and any other external cables or devices connected to the Netgate 8300.

> **Danger: Reminder:**
>
> - Anti-static protection must be used throughout this procedure.

- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Turn power off to the unit by changing the power switch on the rear of the unit to the **off** position.

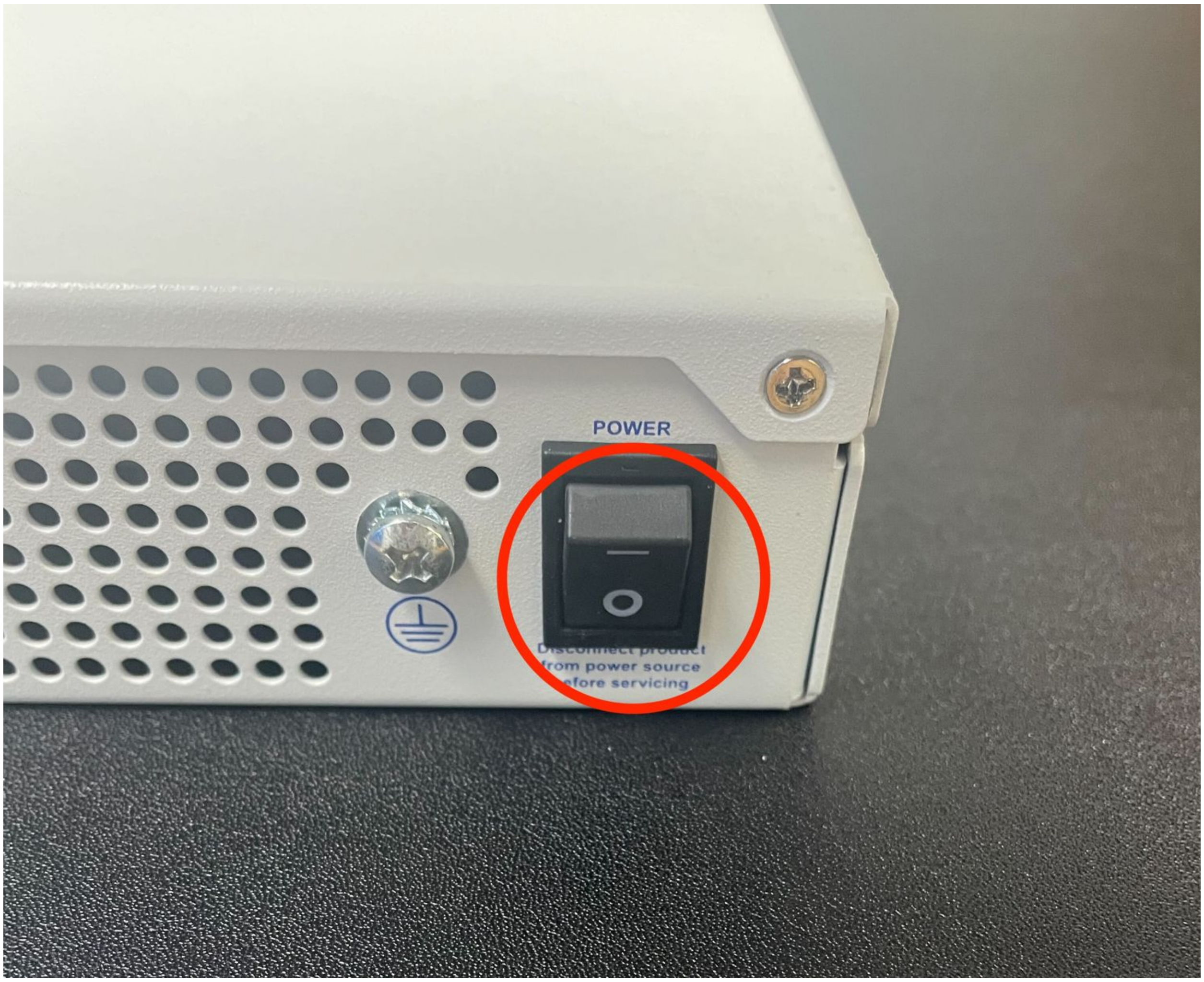


Fig. 1: Power switch (circled) in the off position

2. Unplug the power cables from all installed power supply units (PSUs).

> **Danger:** Wait at least **60 seconds** after unplugging power to proceed. This ensures that all phantom power has dissipated.
>
> The LED indicator on all installed PSUs should be off before proceeding.

3. Unplug all network cables, USB cables and devices, serial console connections, etc.
4. Dismount the Netgate 8300 from the rack
5. Move the Netgate 8300 to a safe work location such as an anti-static mat

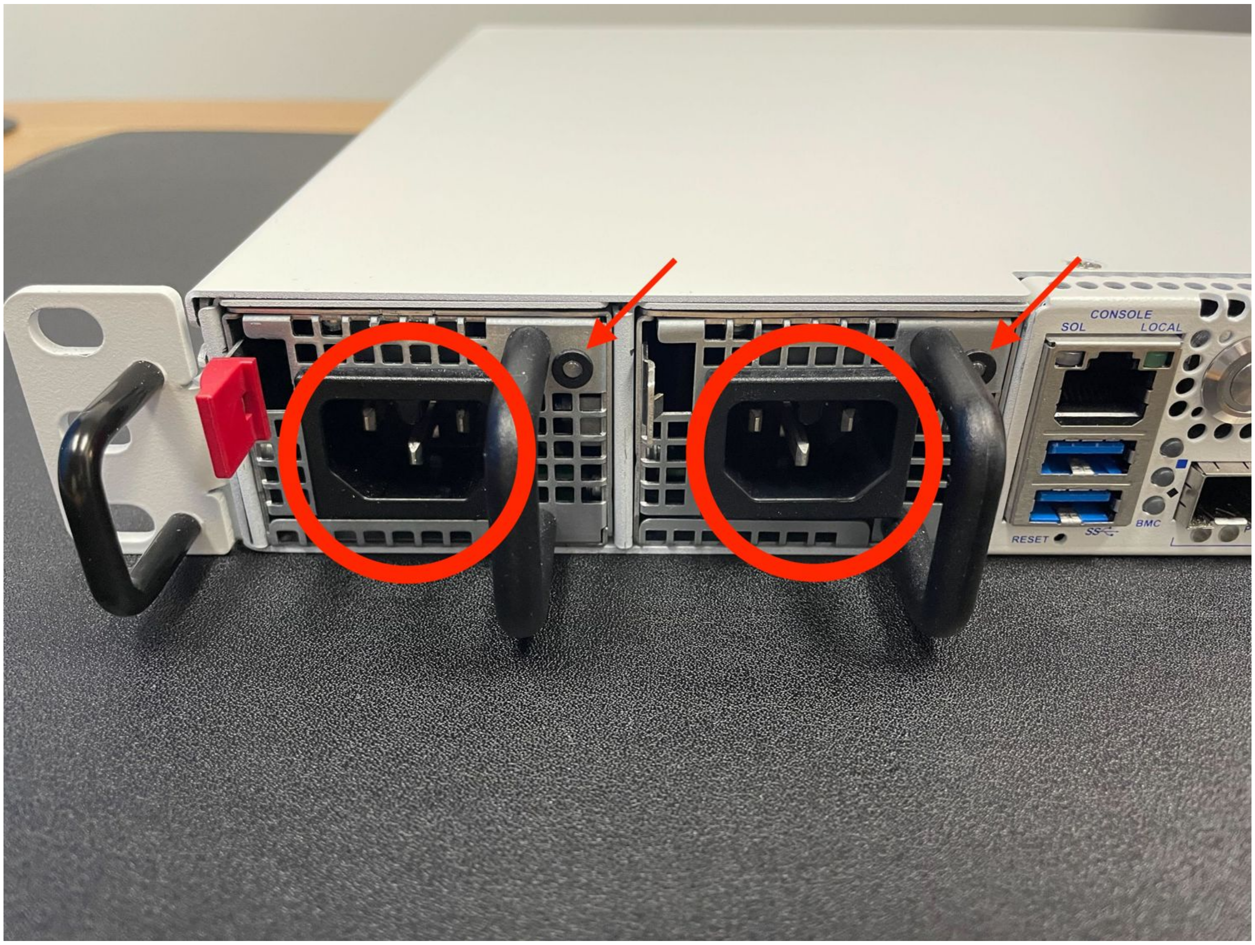


Fig. 2: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

7.3.4 Removing the Lid

The next portion of the procedure involves opening the device and removing the lid.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Remove the screws from the top of the case near the front of the unit using the Phillips head screwdriver.

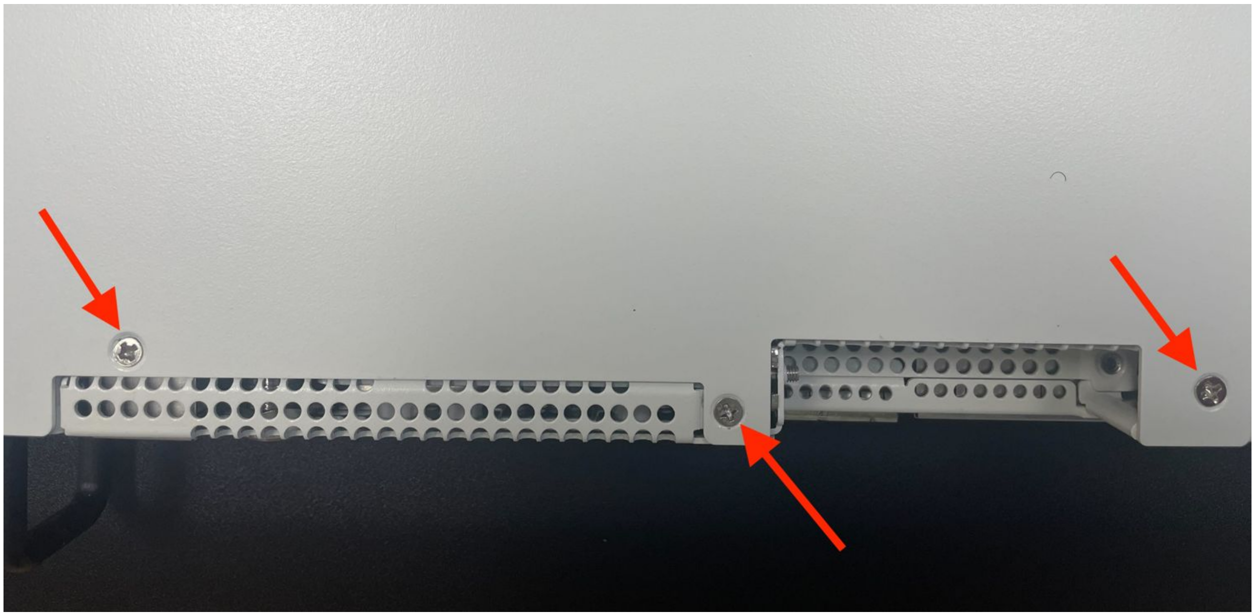


Fig. 3: Screws on the top of the cover at the front of the unit, indicated with arrows

2. Remove the screw from the rear side of the unit at the top left corner using the Phillips head screwdriver.
3. Remove the screw from the rear side of the unit at the top right corner using the Phillips head screwdriver.
4. Slide the top cover back away from the front panel until it stops.
5. Lift off the top cover and set it aside, keeping it upright to avoid damaging the top surface.

7.3.5 Move the Fan Duct

The M.2 NVMe riser card is located under the fan duct. This duct can be moved out of the way sufficiently enough to access the riser without completely removing it from the case.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Remove the screw retaining the side of the fan duct nearest to the PSU cages using the Phillips head screwdriver.

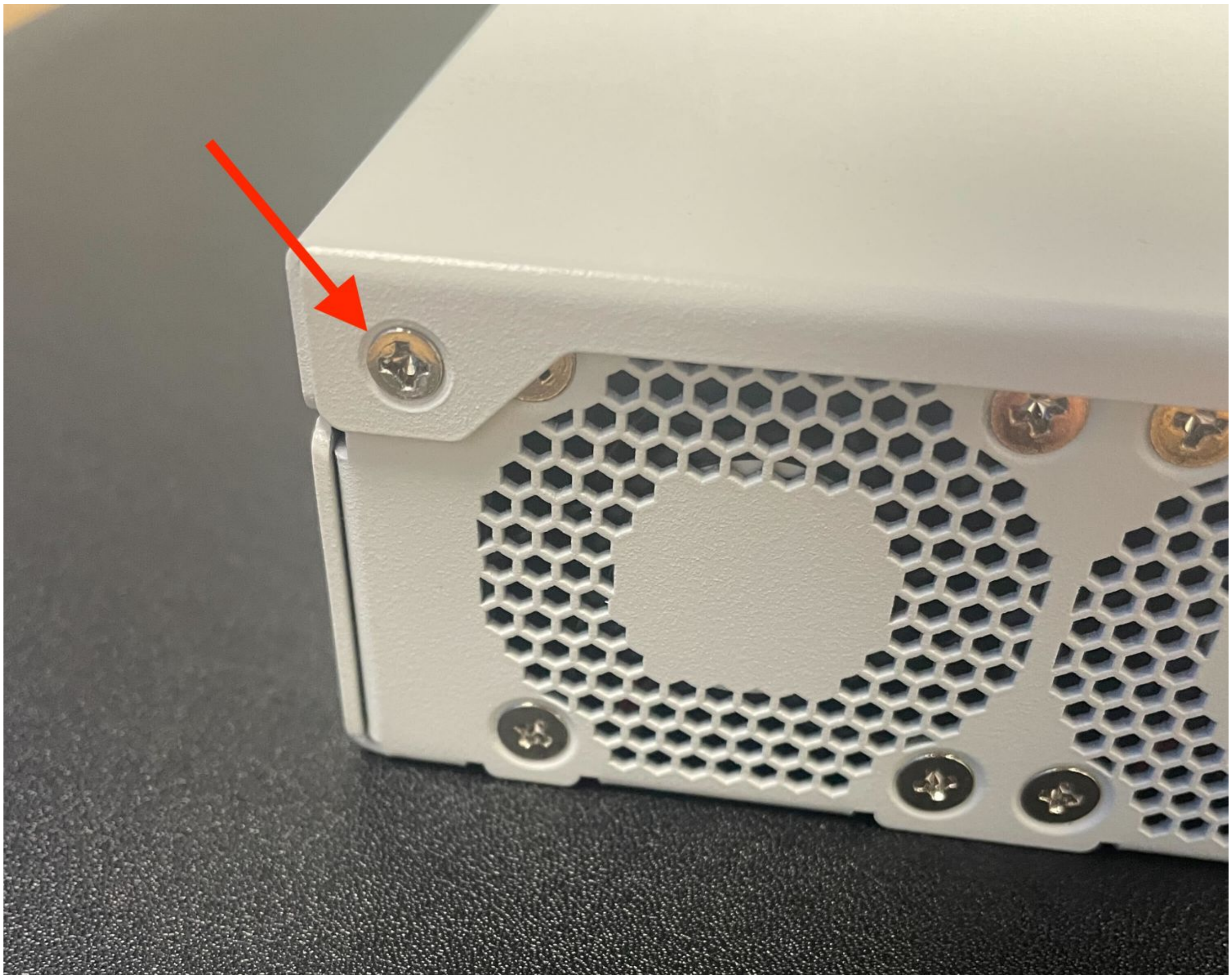


Fig. 4: Screw on the rear side of the unit at the left top corner, indicated with an arrow.

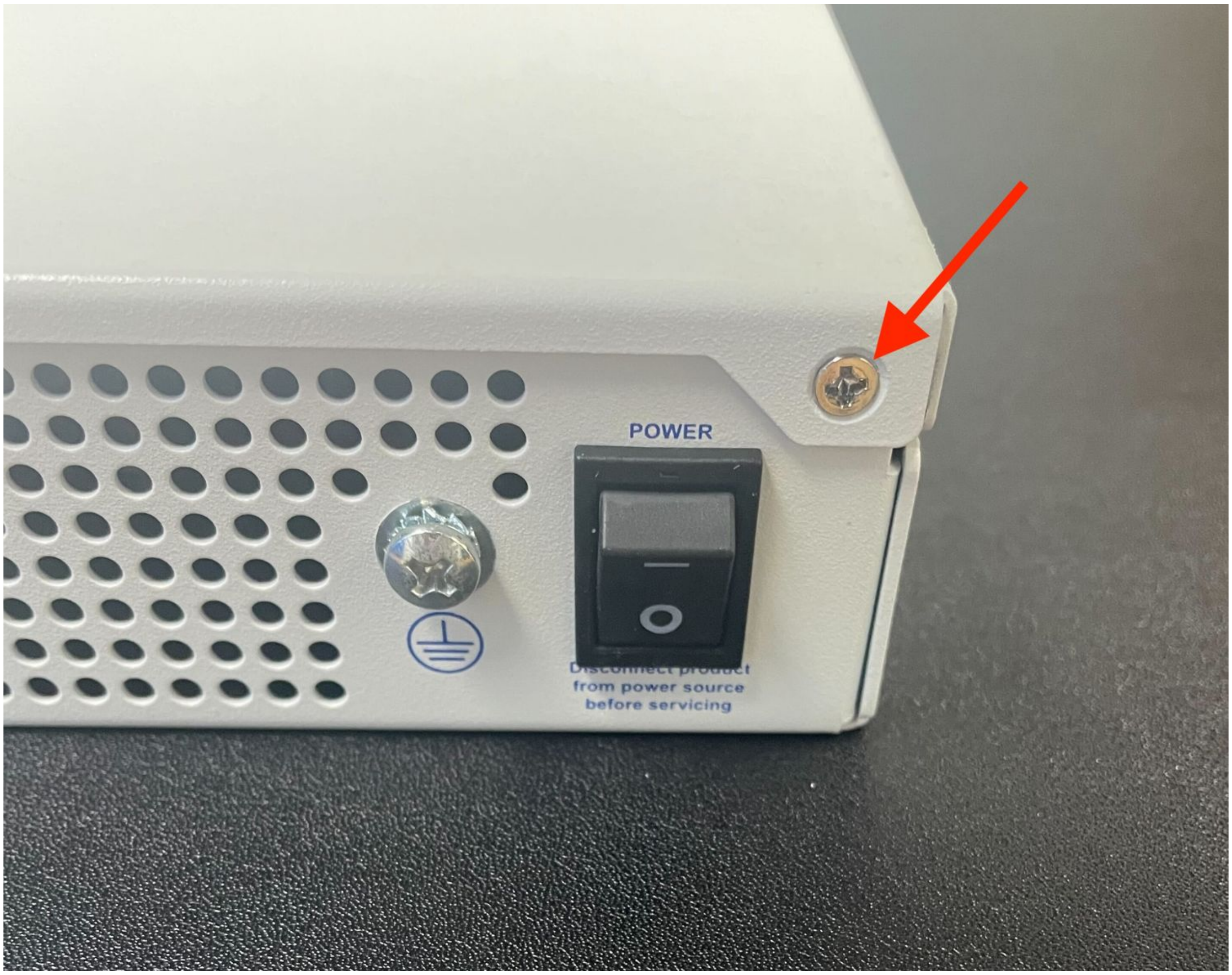


Fig. 5: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

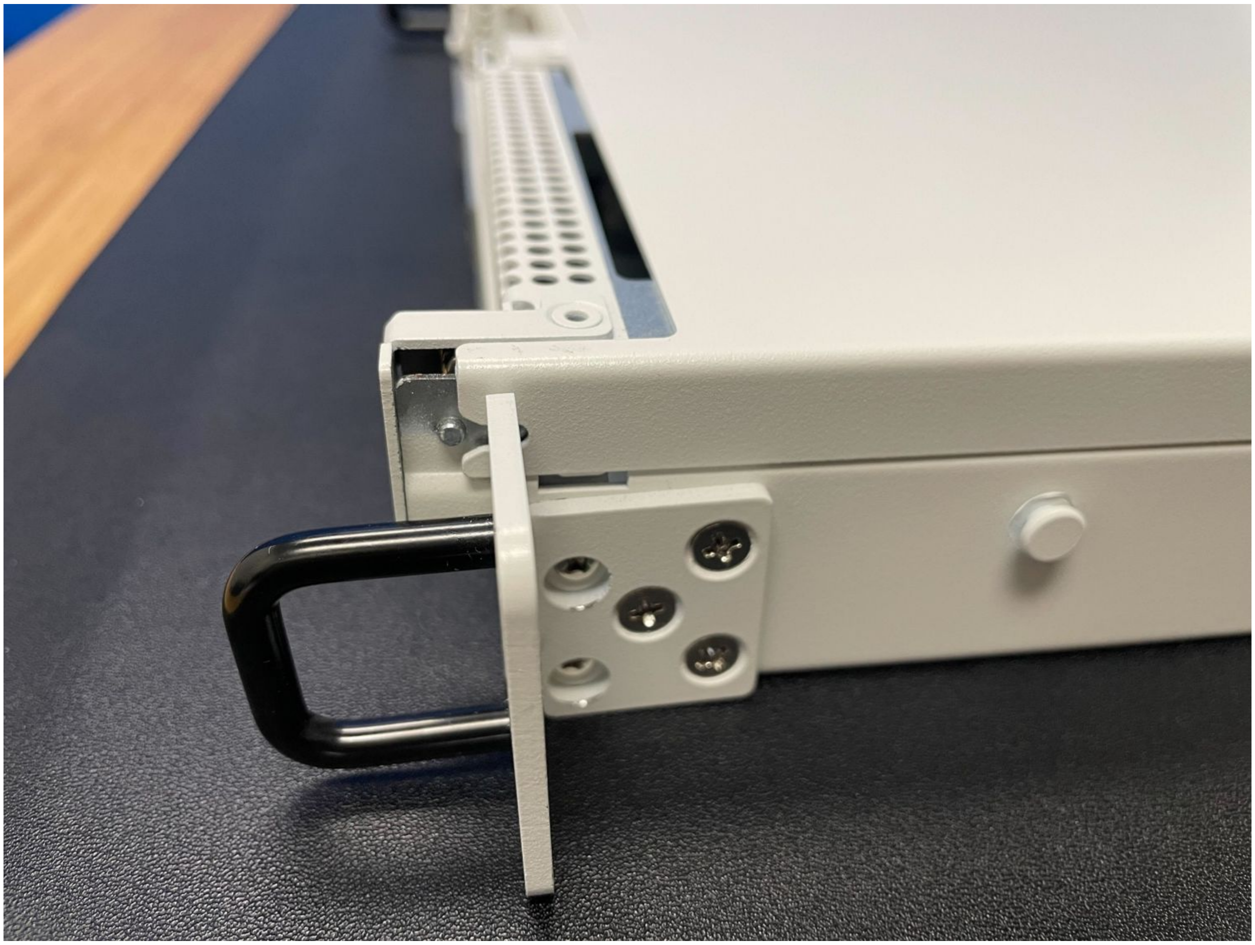


Fig. 6: Sliding back the top cover away from the front panel

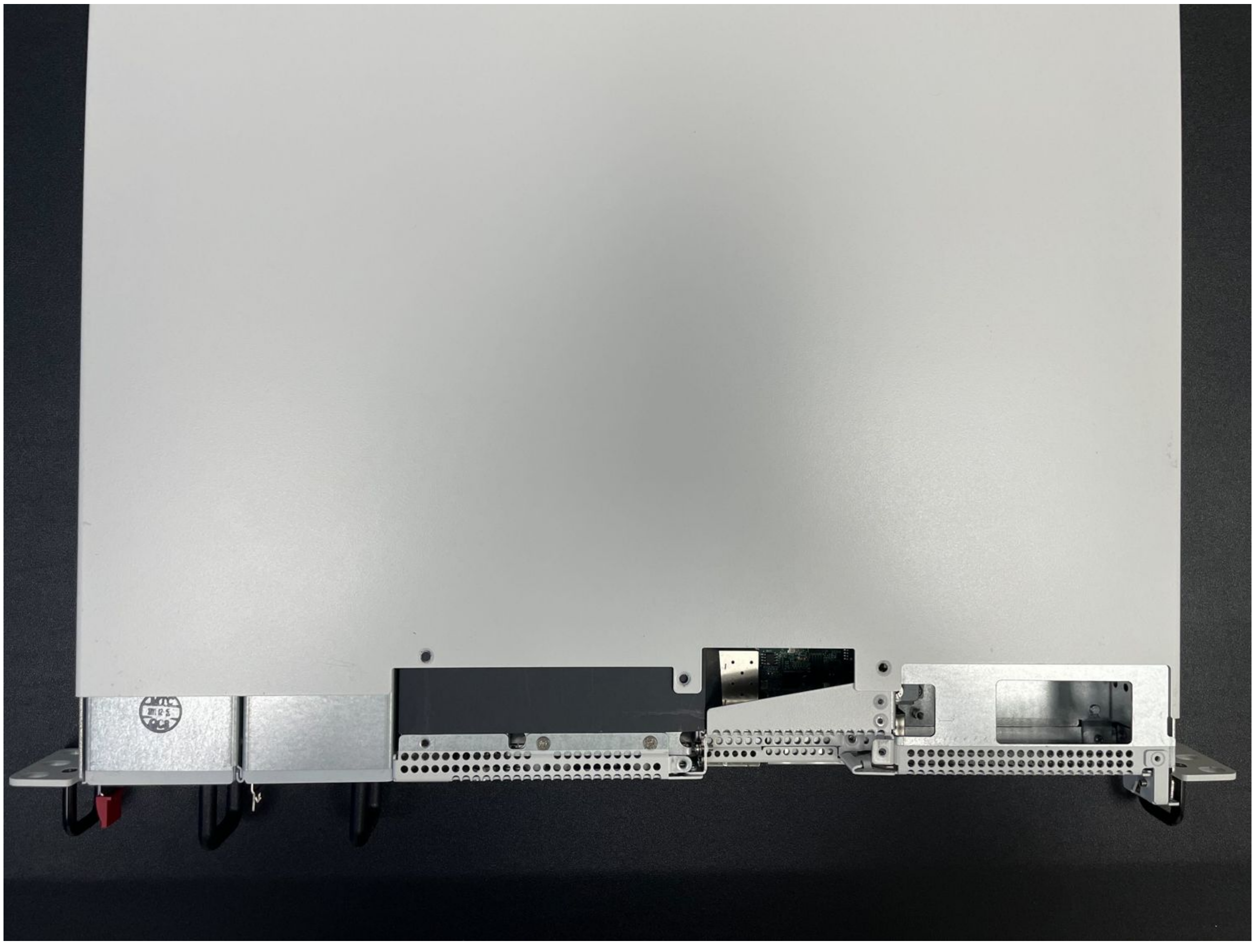


Fig. 7: Top cover in position to be lifted off

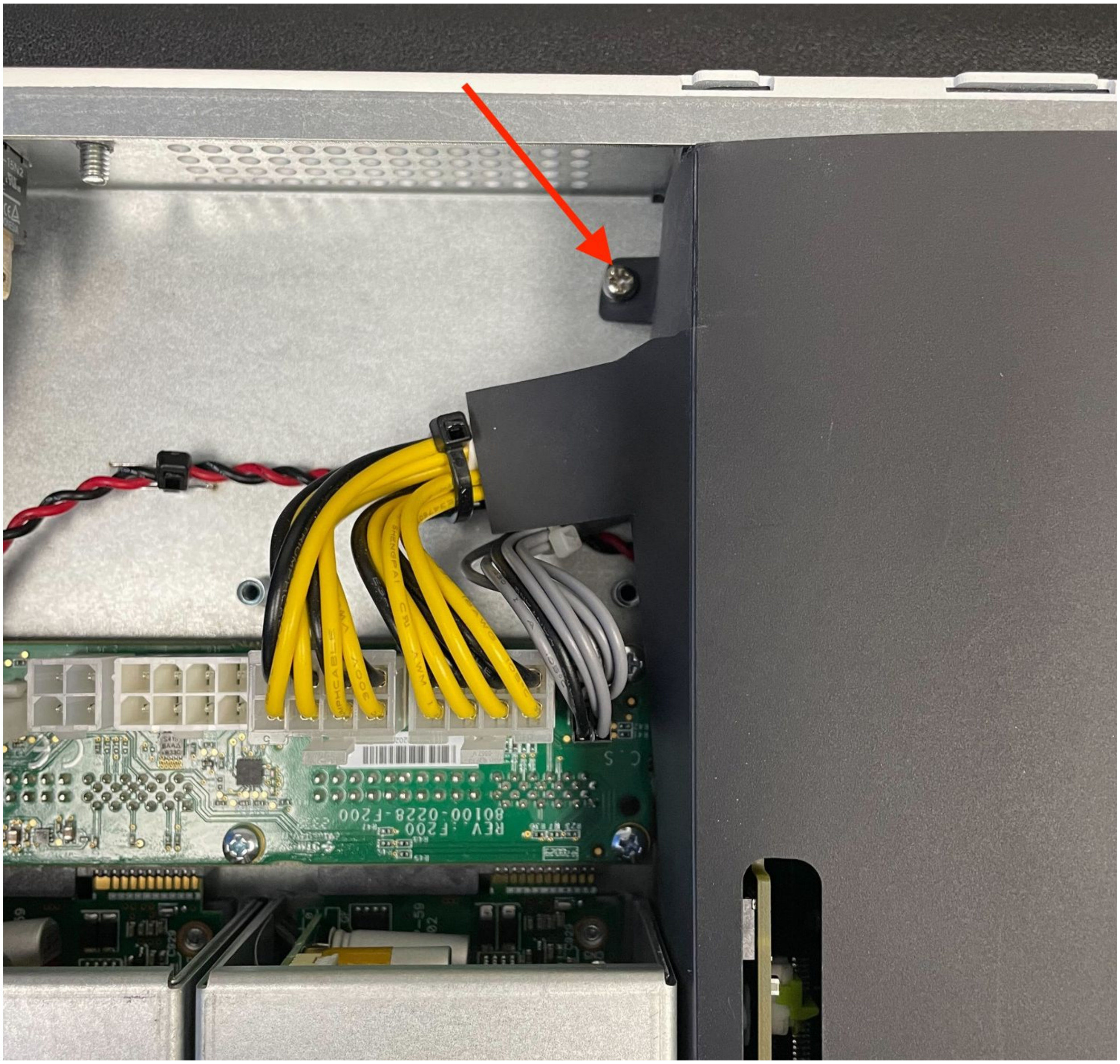


Fig. 8: Screw holding the fan duct in place, indicated with an arrow

2. Gently lift the side of the fan duct up and out of the way

7.3.6 Remove the M.2 NVMe Riser Card

The M.2 NVMe drives are located on a riser card near the PSU cages. This card must be removed to safely access the SSDs.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Locate the M.2 NVMe riser card
2. Lift both retaining clips holding the riser card in place to release the card
3. Remove the riser card and set it aside

7.3.7 Install the SSD

With the riser card removed, it is time to install the SSD.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Turn the riser card over so the second M.2 slot is visible.

   Note: As mentioned earlier in this document, the Netgate 8300 currently supports M.2 B+M-Key or M-Key PCIe NVMe SSDs in 2280 or 2242 sizes.

2. Move the retainer clip to match the SSD size being installed.

   The M.2 slot accepts both 2280 and 2242 size cards, but the device ships with the retaining clip set for a 2280 size card by default.

   This clip can easily be moved to accommodate a 2242 card without any tools.

   If the card being installed is a 2280 size card, these steps are unnecessary.

   1. Rotate the retaining clip 90 degrees counterclockwise to release it.
   2. Lift the retaining clip away from the riser.
   3. Insert the retaining clip in the 2242 position hole outlined in white on the riser.
   4. Rotate the retaining clip 90 degrees clockwise to lock it in place.

3. Insert the M.2 card into the empty socket at an approximate 30° angle

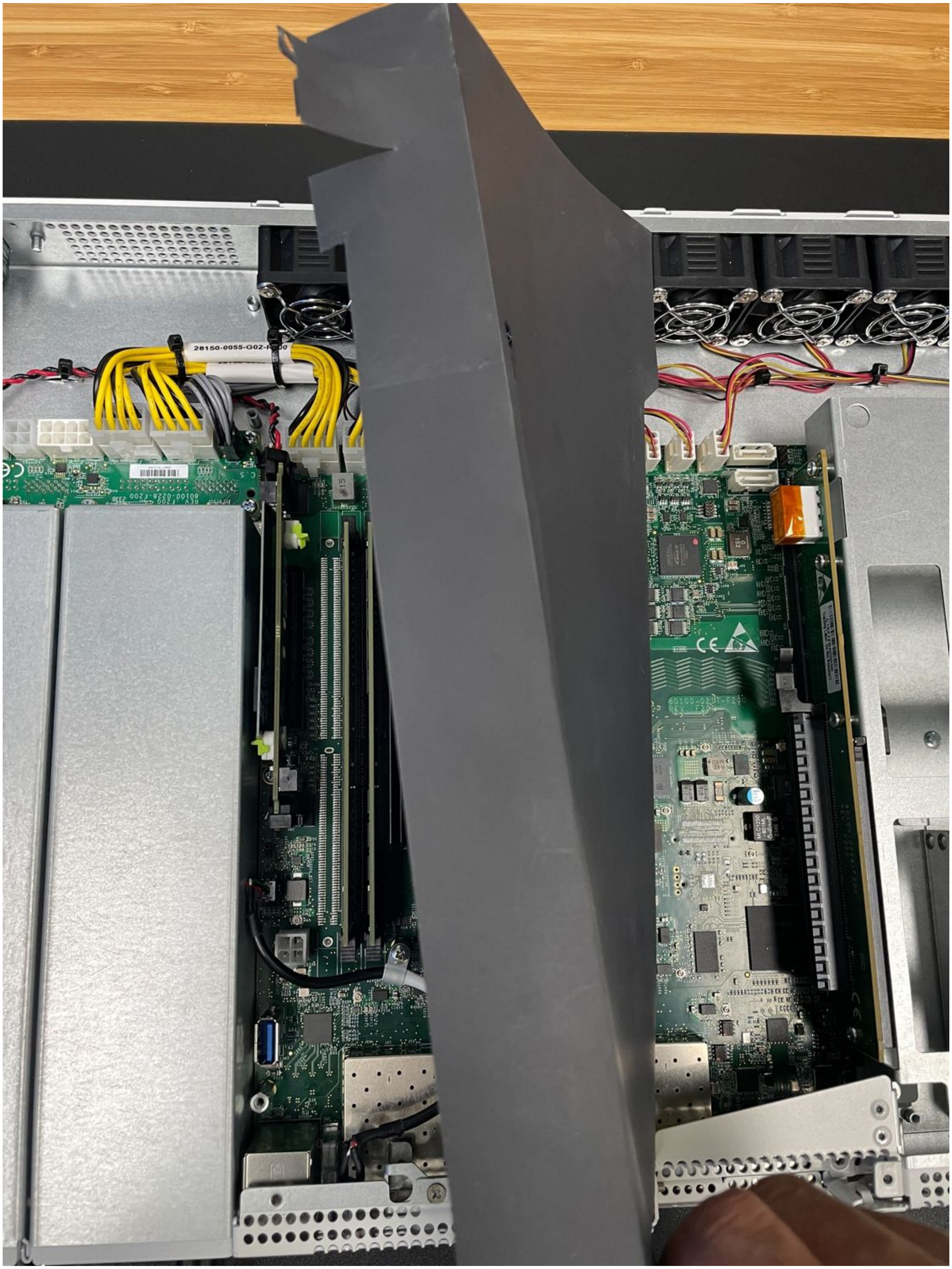


Fig. 9: Fan duct lifted out of the way to access the M.2 NVMe riser

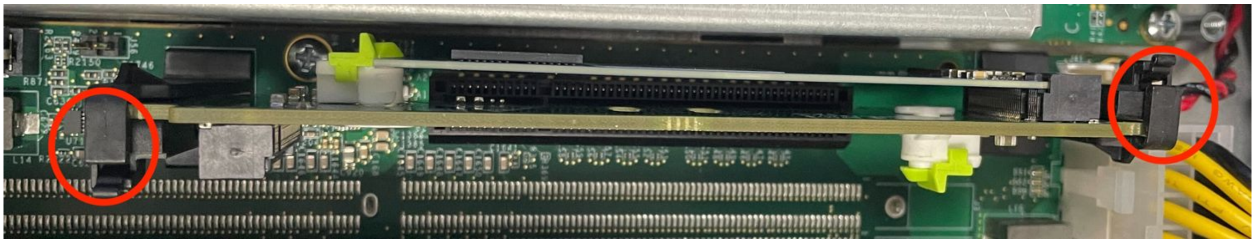


Fig. 10: M.2 NVMe riser card clips (circled) in the closed position

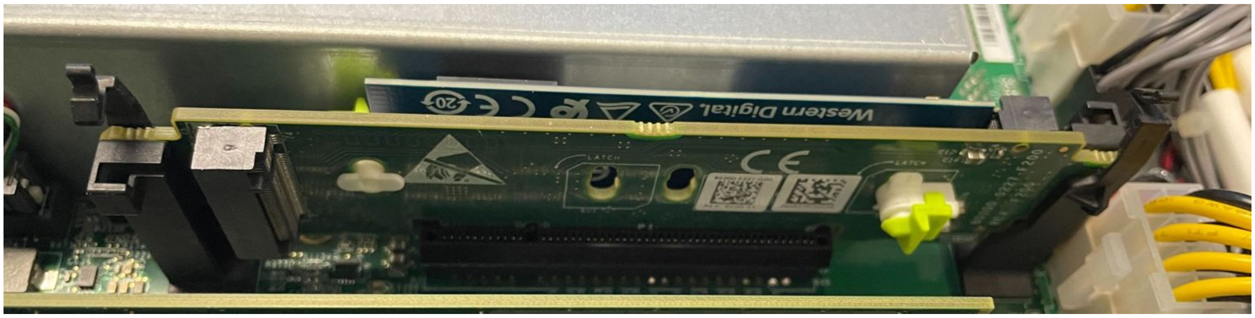


Fig. 11: M.2 NVMe riser card clips in the open position

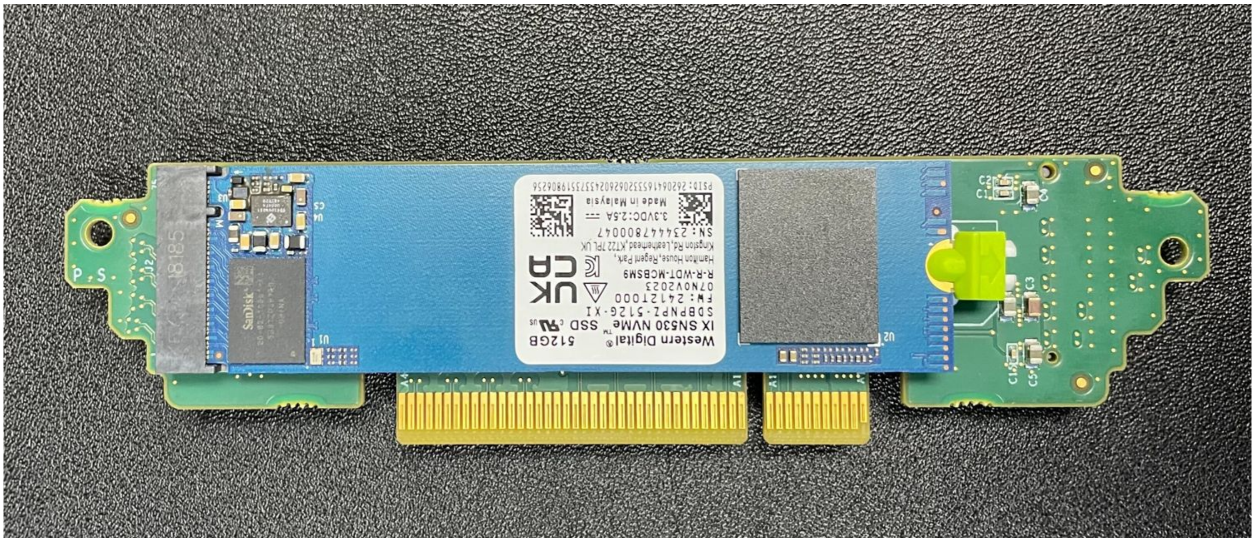


Fig. 12: M.2 NVMe riser card slot 1 with the stock SSD installed

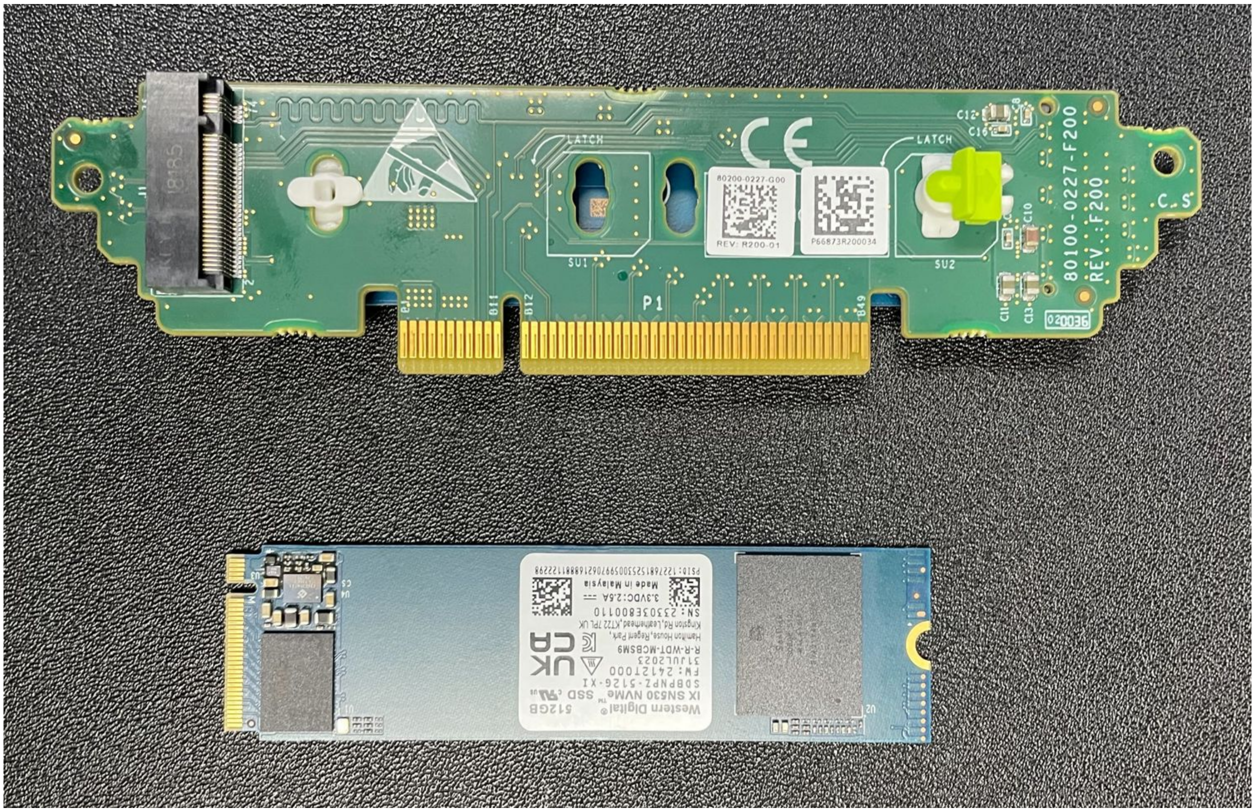


Fig. 13: M.2 NVMe riser card slot 2 (empty) and add-on M.2 NVMe SSD before install

Warning: M.2 cards are keyed. **Do not** force an M.2 card into a slot with mismatched keying.

Refer to M.2 Edge Connector Keying for a depiction of the different M.2 key types.

4. Gently push down the M.2 NMVe card until it snaps into place against the retaining clip.

   There should be an audible "snap" sound as the retaining clip locks the drive into position.

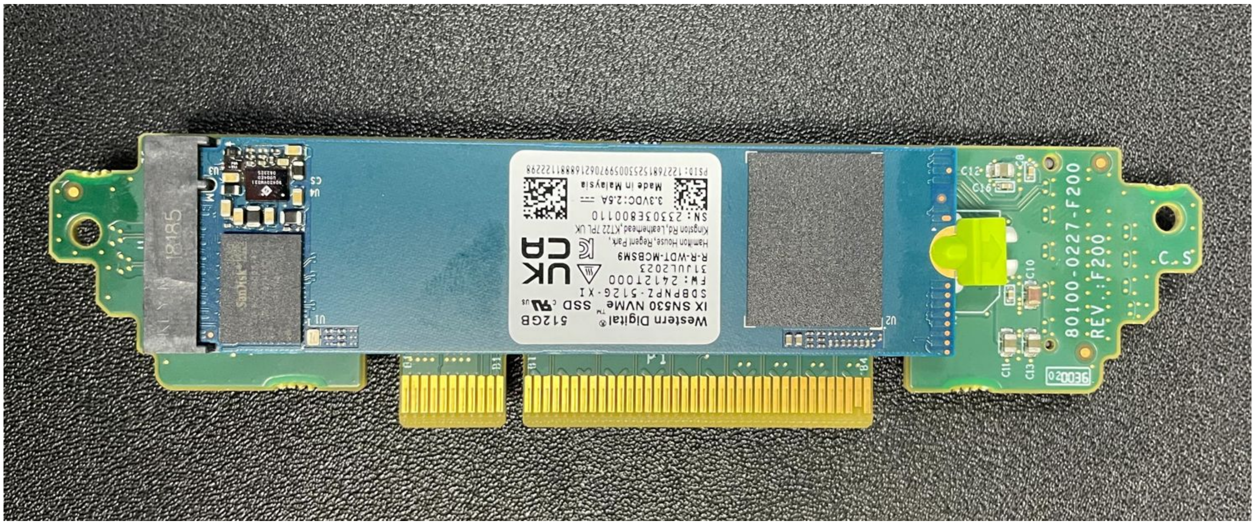


Fig. 14: M.2 NVMe riser card slot 2 with the add-on SSD installed

Danger: Ensure that the retaining clip is fully engaged to avoid damaging the SSD!

7.3.8 Replace the M.2 NVMe Riser Card and Fan Duct

With the new SSD installed, replace the riser card.

Danger: **Reminder:**

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Insert the riser card back into its slot on the motherboard
2. Close the retaining clips to secure the riser card.
3. Move the fan duct back to its original location.
4. Secure the fan duct with its screw using the Phillips head screwdriver.

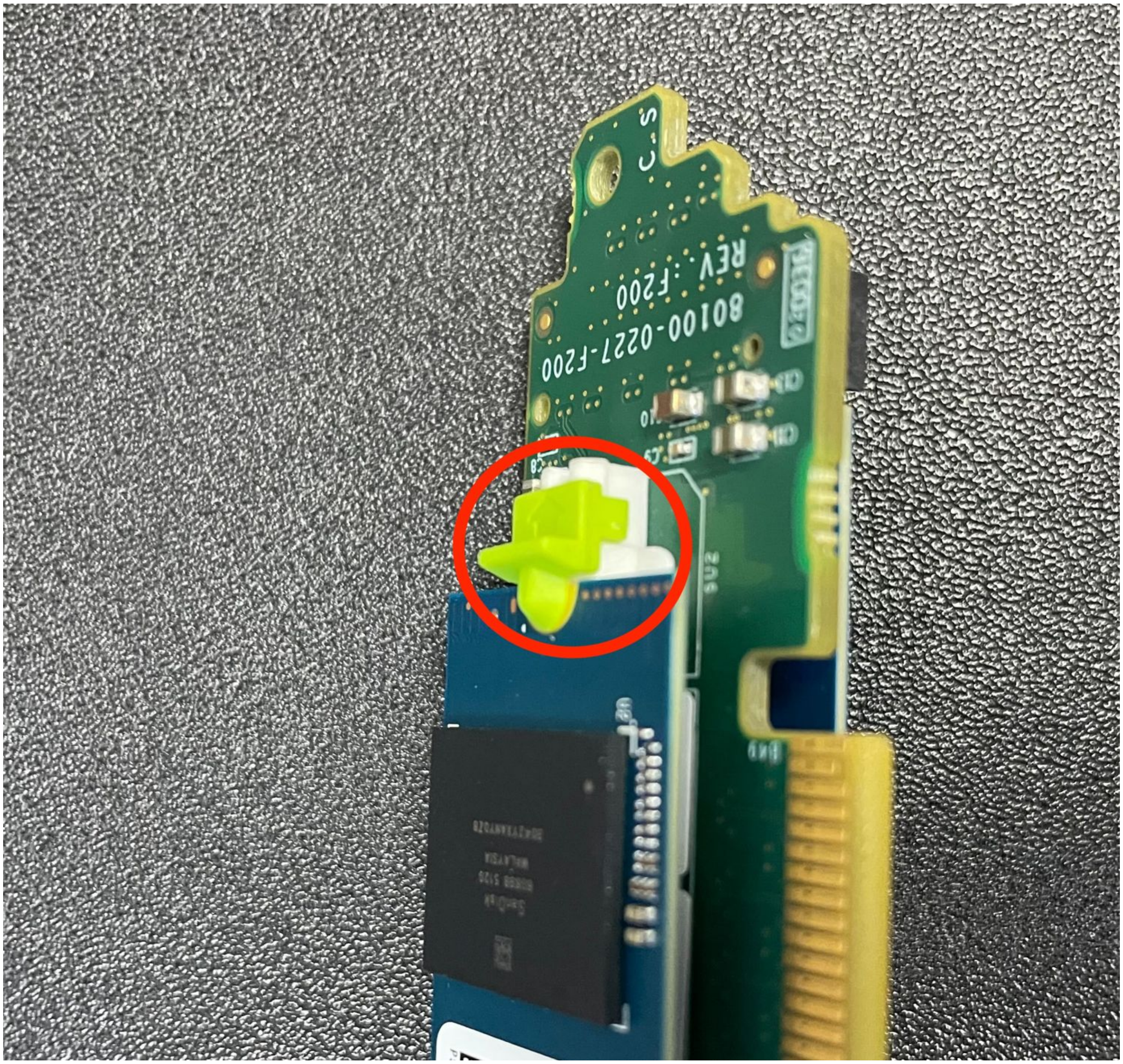


Fig. 15: Close-up view of the M.2 retaining clip for slot 2 with the SSD secured

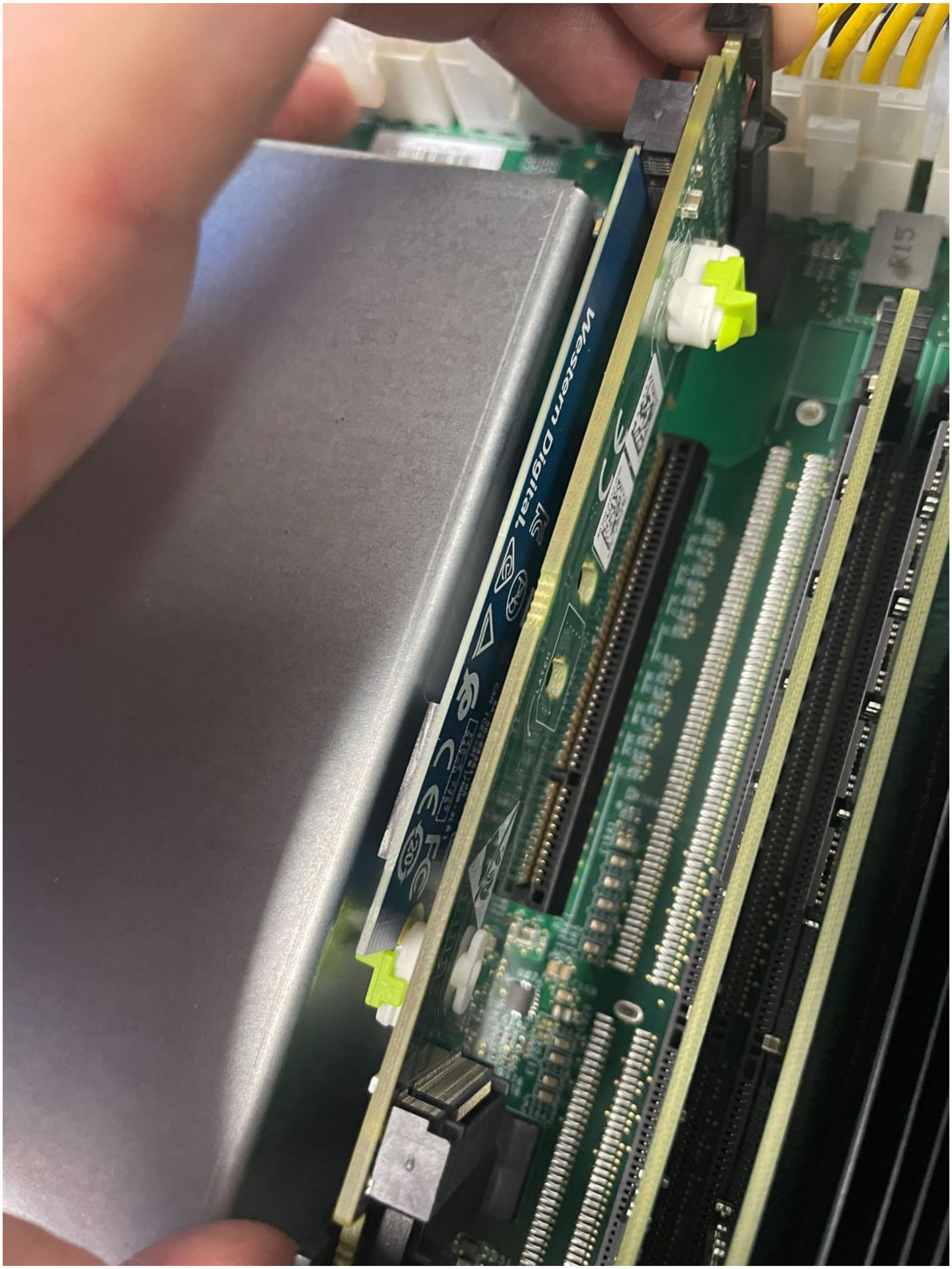


Fig. 16: Replacing the M.2 riser card

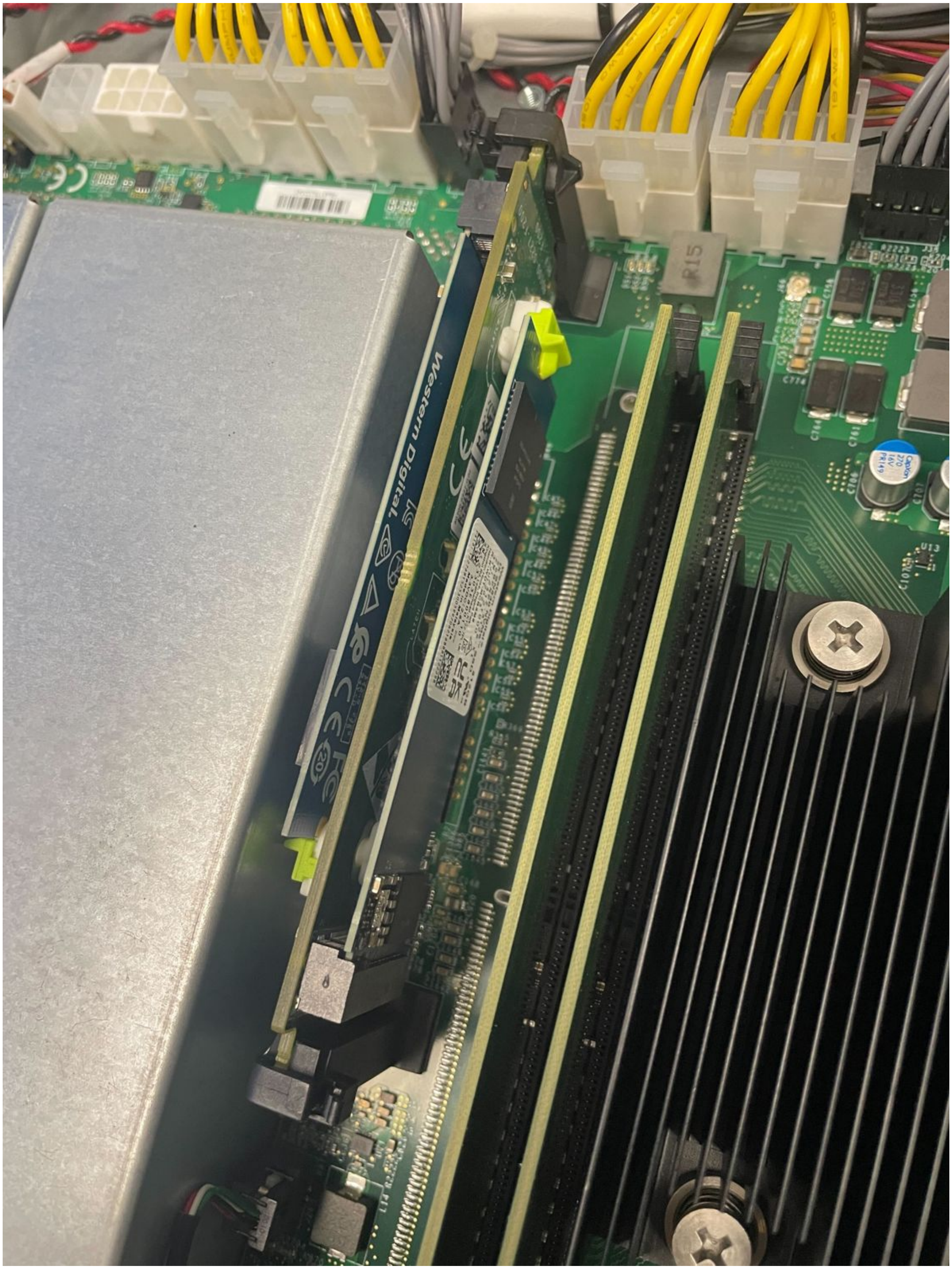


Fig. 17: M.2 riser card with two SSDs and riser clips in the closed position

7.3.9 Replacing and Fastening the Lid

With the internal components all in place, the next step is to replace the lid and all its fasteners.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Align the top cover with the top of the unit, a short distance behind the front panel.

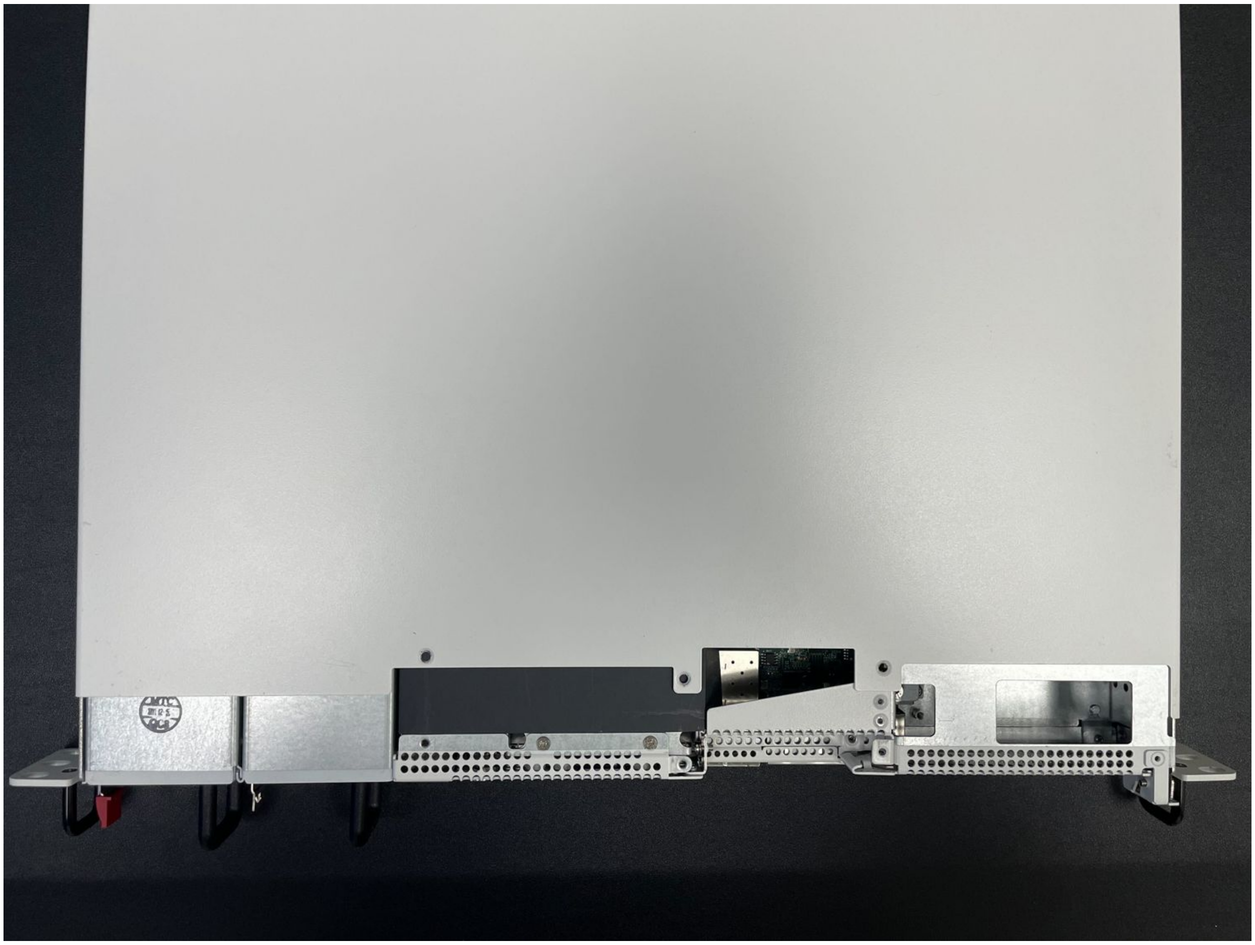


Fig. 18: Top cover in position to be replaced

2. Slide the top cover toward the front of the unit into its closed position.

# Replace the screws on the rear of the unit (left and right top corners) using
the Phillips head screwdriver.

# Replace the screws on the top of the unit using the Phillips head screwdriver.

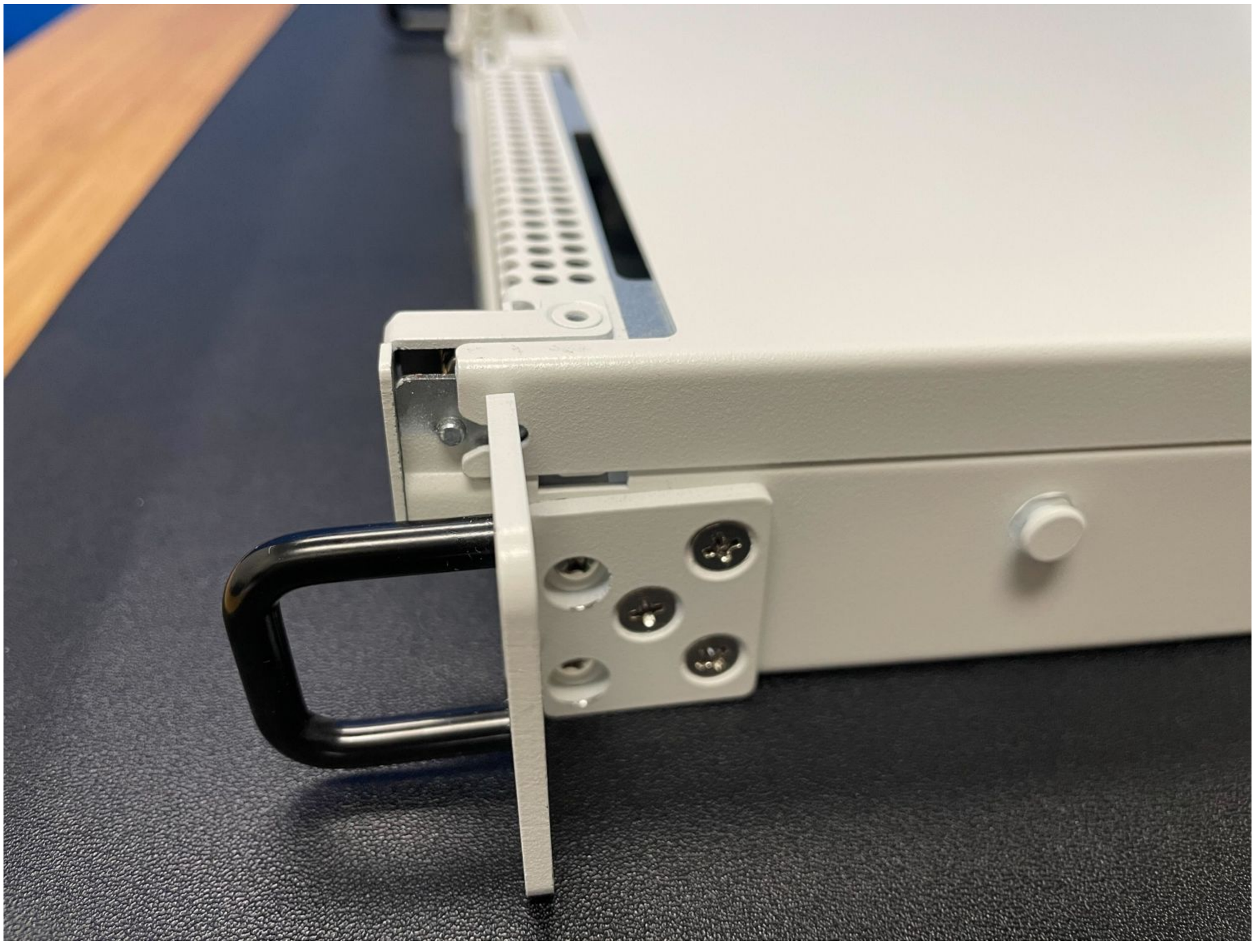


Fig. 19: Slide the top cover back toward the front panel

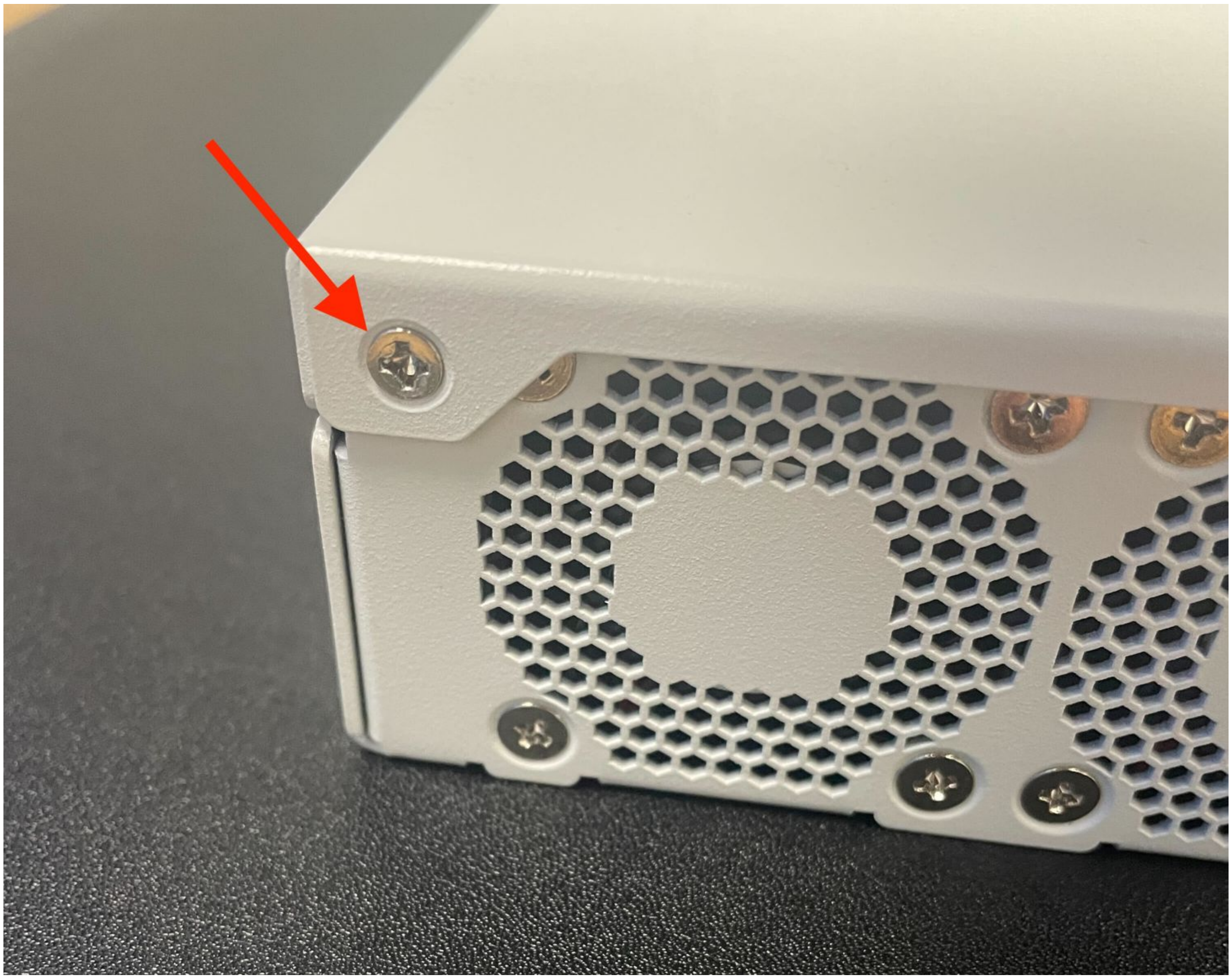


Fig. 20: Screw on the rear side of the unit at the left top corner, indicated with an arrow.

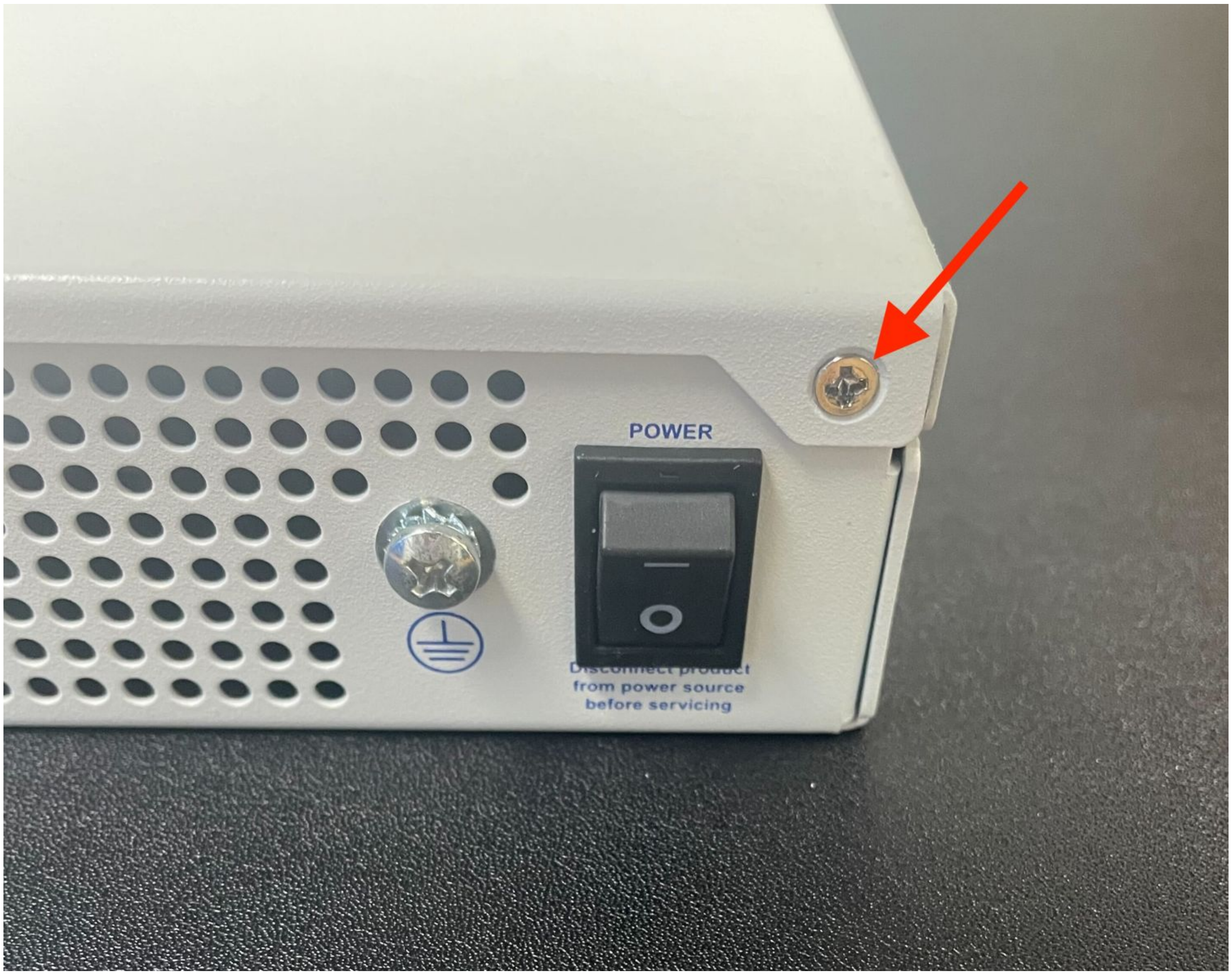


Fig. 21: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

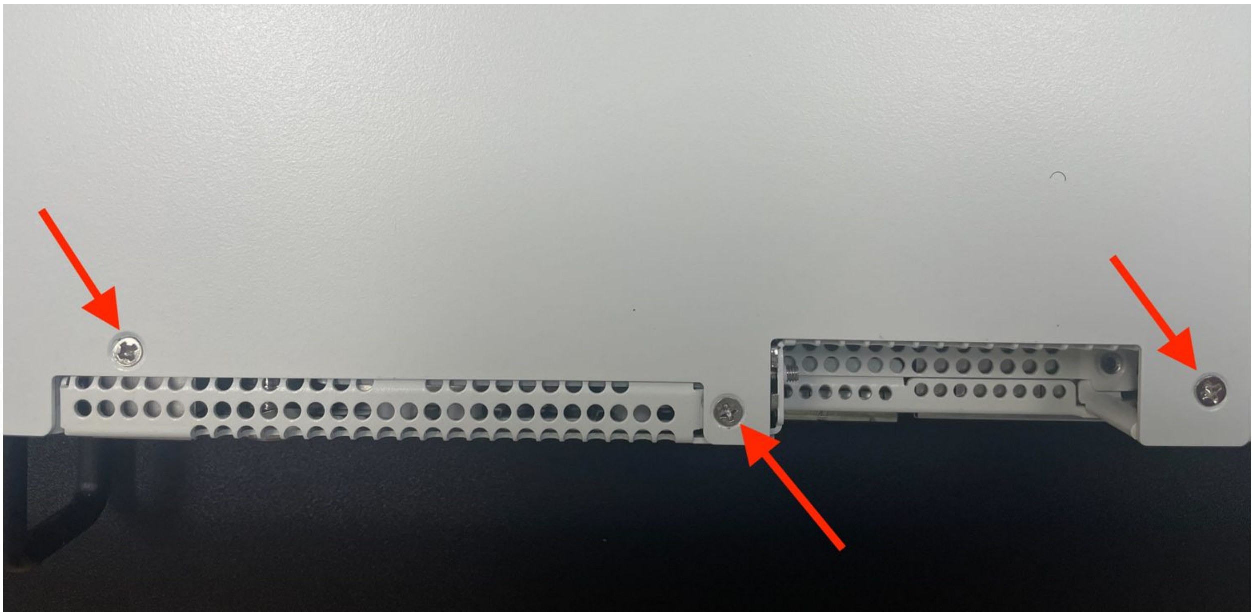


Fig. 22: Screws on the top of the cover at the front of the unit, indicated with arrows

7.3.10 Reconnect

The device is now ready to be put back into its former location.

1. Mount the Netgate 8300 in the rack
2. Plug in all network cables, USB cables and devices, serial console connections, etc.
3. Insert the USB memstick containing the installation media
4. Plug the power cables into all installed power supply units.
5. Turn power on to the unit by changing the power switch on the rear of the unit to the **on** position.
6. Reconnect to the serial console

7.3.11 Reinstall TNSR Software

Note: This section assumes the new disk will be used as a part of a mirrored disk pair using software RAID. If the new disk is for additional storage, consult the operating system documentation for instructions on formatting and mounting an additional disk.

With the device back together and ready to proceed, the next step is to reinstall TNSR software using the new SSD and the existing SSD as a software RAID mirror.

Warning: This action requires reformatting the existing drive and reinstalling TNSR software. All data on the existing installation will be lost, so backup any important data before proceeding.

Follow the procedure in Installing TNSR Using Software RAID to complete the setup.

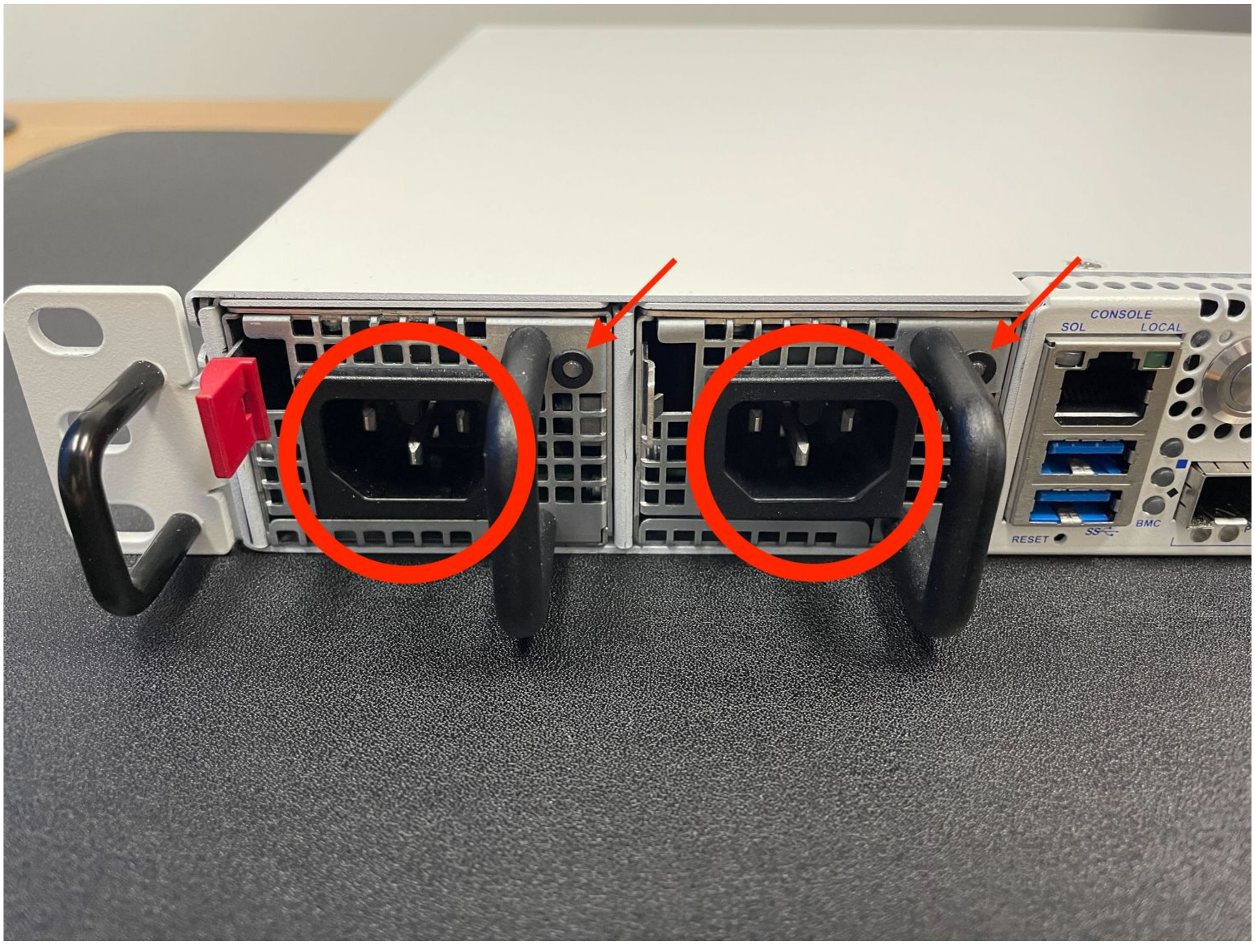


Fig. 23: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

7.3.12 Restore the Configuration

If a configuration was *backed up earlier in this procedure*, now is the time to restore the configuration using the method described in the TNSR software documentation section on Backup and Restore.

7.3.13 Re-arm the Intrusion Sensor

Opening the case to install the new drive will have triggered the intrusion alarm sensor, even when the device was removed from power. The intrusion alarm causes the fans to run at a higher fixed speed until the sensor is re-armed.

Once TNSR software is up and running, follow the procedure in *Re-arm the Chassis Intrusion Switch* to reset the sensor.

CHAPTER

EIGHT

ADD-ON EXPANSION CARD INSTALLATION

The Netgate® 8300 has two expansion card slots available for additional devices such as 25 Gbit/s or 100 Gbit/s network interface cards.

The two expansion card slots have the following capabilities:

- 1x PCIe 3.0 x8 LP (Low Profile) slot which supports half-length low profile cards.
- 1x PCIe 4.0 x16 slot which supports full-height three-quarter length cards.

See also:

See *Input and Output Ports* for additional information on the expansion card slots.

Add-On Expansion Card Installation Outline

8.1 Warnings and Precautions

Danger: **Anti-static protection must be used throughout this procedure**.

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and add-on cards. There are many delicate components which can be damaged during this process. **Damage caused via physical contact and electrostatic discharge while performing this installation is not covered by the warranty**.

Warning: This device includes an intrusion detection sensor which operates even when the device is without power.

Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in *Re-arm the Chassis Intrusion Switch*.

When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

8.2 Required Tools and Hardware

Installing add-on expansion cards in the Netgate 8300 requires the following tools and hardware:

- Phillips screwdriver
- Anti-static grounding strap and anti-static mat for handling bare components and the 8300 system
- Compatible expansion card

8.3 Installation Procedure

The installation procedure has many steps which are broken down into related groups in the remainder of this document. Follow all steps in the procedure carefully.

8.3.1 Take a Backup

If the system contains an existing configuration, then the first step is to take a backup of that configuration for safety.

If the existing configuration is not necessary, this section may be skipped.

There are numerous backup options covered in the TNSR software documentation section on Backup and Restore.

8.3.2 Power Off and Disconnect

Installing an add-on expansion card requires removing the top of the case to expose the internal components. For safety, before opening the case, the Netgate 8300 must be **completely** disconnected from everything. This includes power, network cables, USB cables, serial console cables, and any other external cables or devices connected to the Netgate 8300.

> **Danger: Reminder:**
>
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Turn power off to the unit by changing the power switch on the rear of the unit to the **off** position.
2. Unplug the power cables from all installed power supply units (PSUs).

   > **Danger:** Wait at least **60 seconds** after unplugging power to proceed. This ensures that all phantom power has dissipated.
   >
   > The LED indicator on all installed PSUs should be off before proceeding.

3. Unplug all network cables, USB cables and devices, serial console connections, etc.
4. Dismount the Netgate 8300 from the rack
5. Move the Netgate 8300 to a safe work location such as an anti-static mat

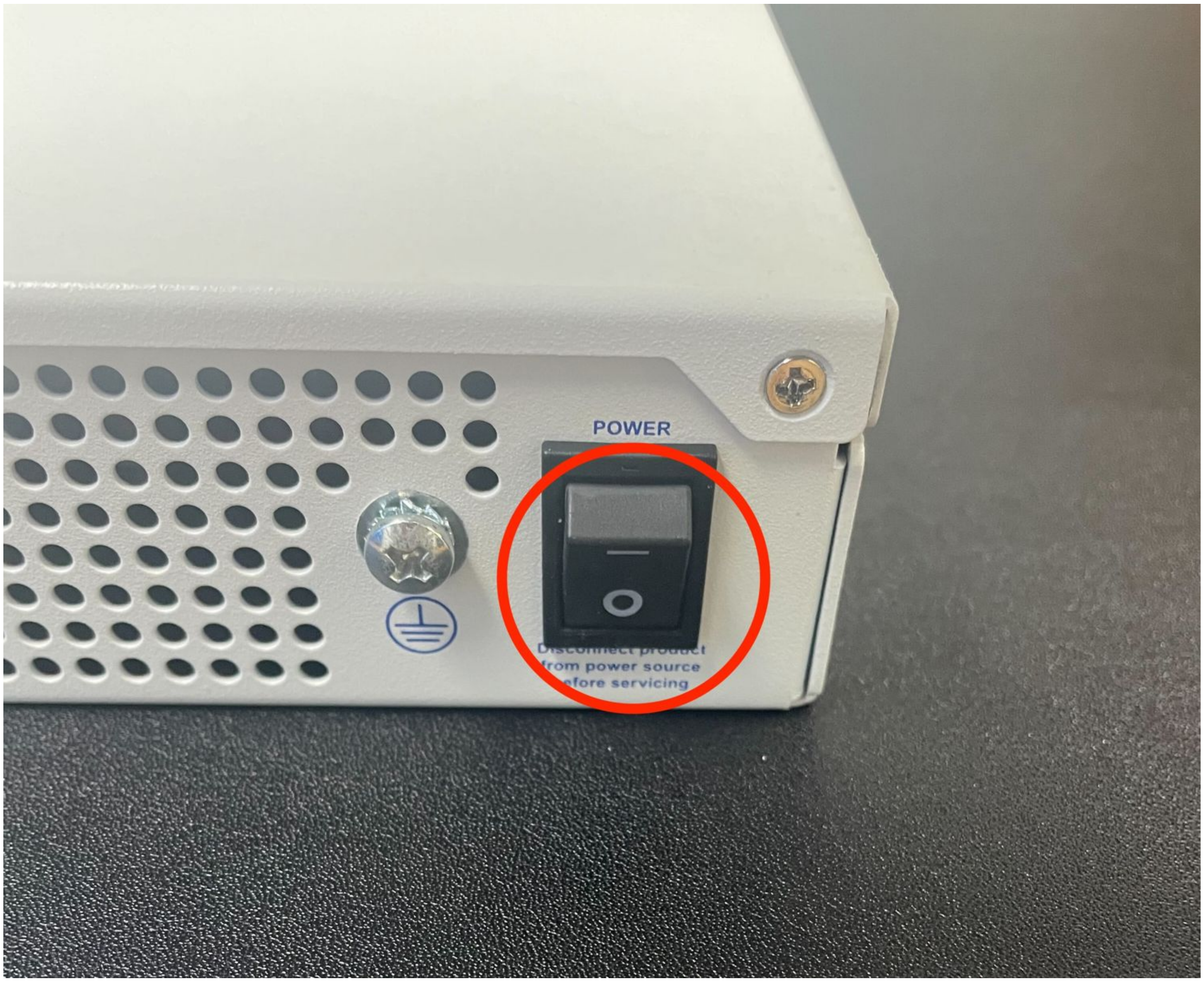


Fig. 1: Power switch (circled) in the off position

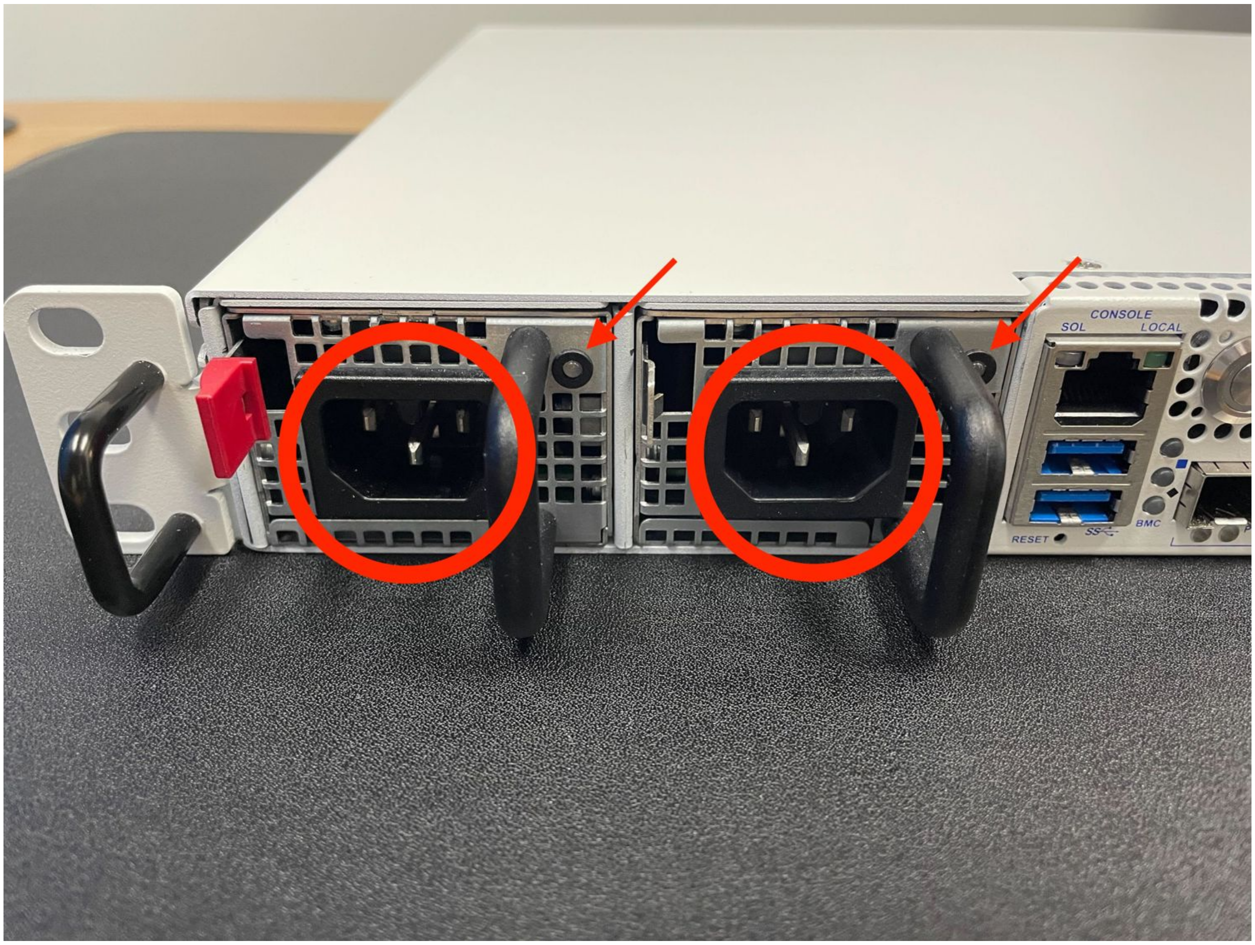


Fig. 2: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

8.3.3 Removing the Lid

The next portion of the procedure involves opening the device and removing the lid.

> **Danger: Reminder:**
>
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Remove the screws from the top of the case near the front of the unit using the Phillips head screwdriver.

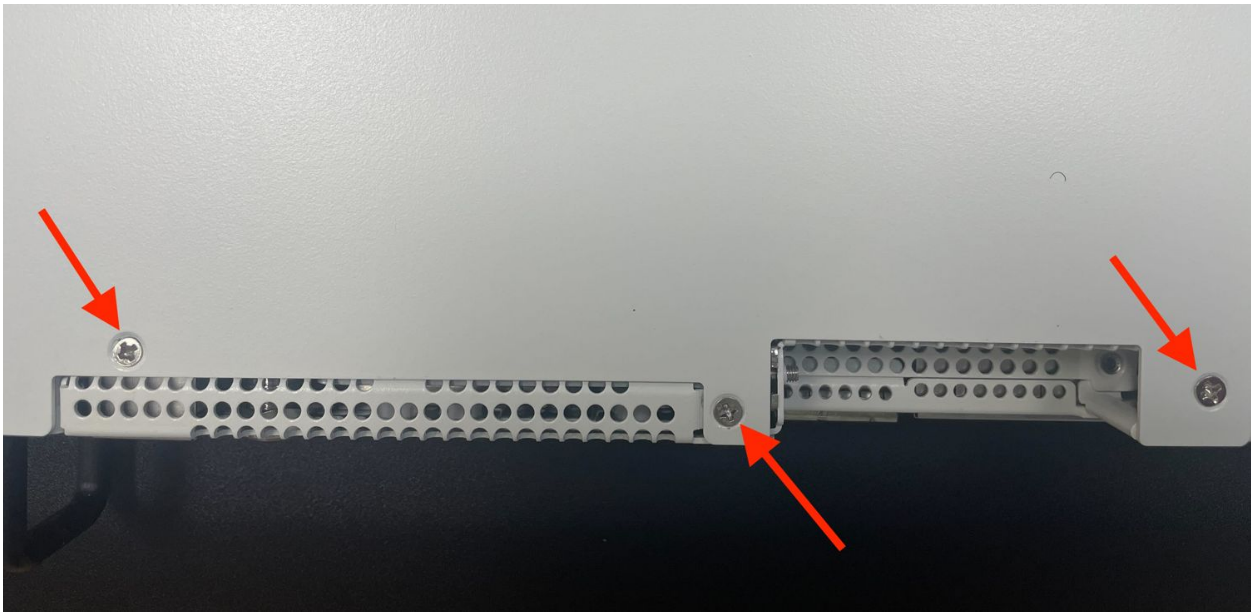


Fig. 3: Screws on the top of the cover at the front of the unit, indicated with arrows

2. Remove the screw from the rear side of the unit at the top left corner using the Phillips head screwdriver.
3. Remove the screw from the rear side of the unit at the top right corner using the Phillips head screwdriver.
4. Slide the top cover back away from the front panel until it stops.
5. Lift off the top cover and set it aside, keeping it upright to avoid damaging the top surface.

8.3.4 Remove the Expansion Riser Assembly

The add-on expansion card slots are located on a riser assembly. This riser assembly must be removed from the device to safely add or remove expansion cards.

> **Danger: Reminder:**
>
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Loosen the two captive screws which attach the riser assembly to the motherboard using the Phillips head screwdriver.

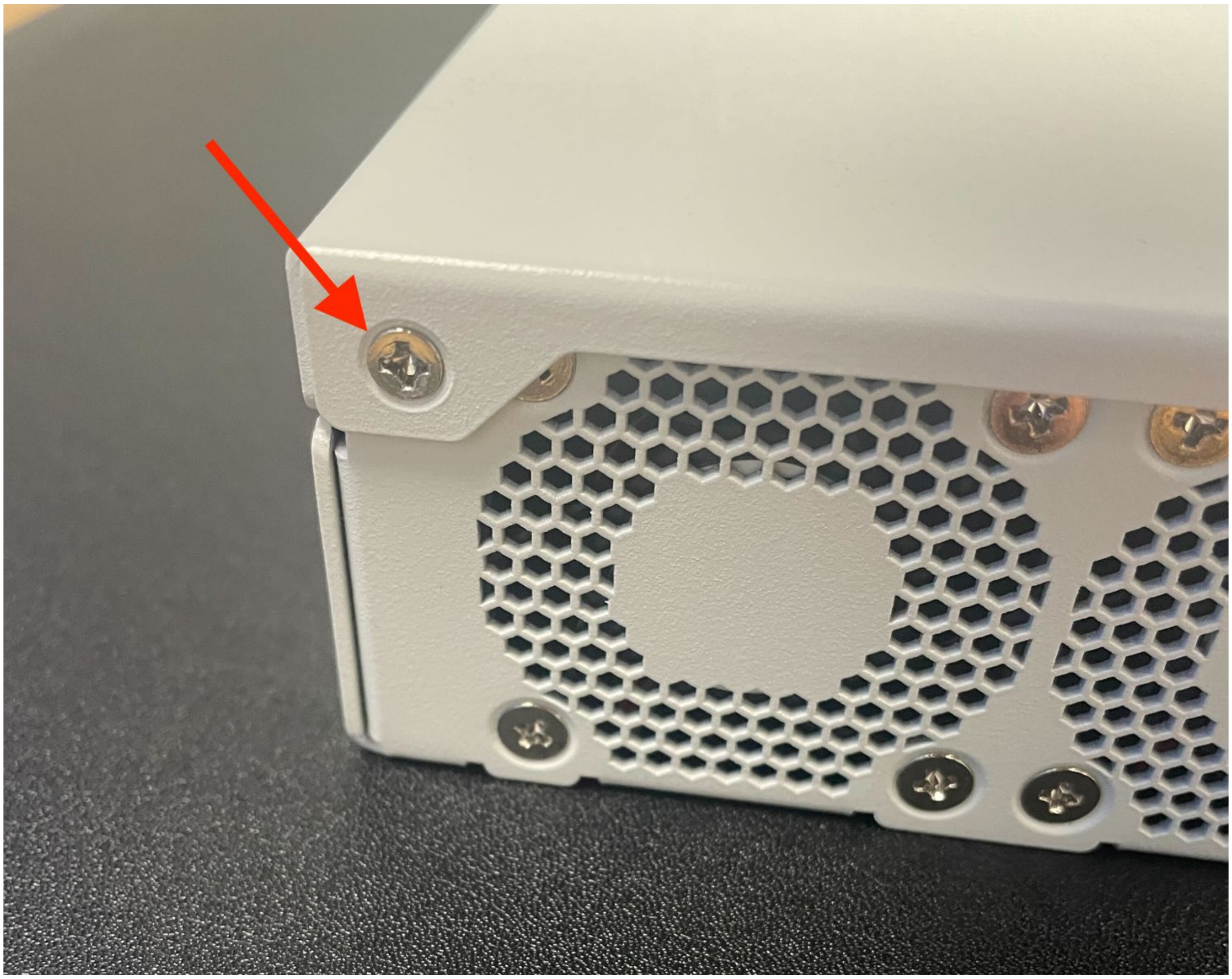


Fig. 4: Screw on the rear side of the unit at the left top corner, indicated with an arrow.

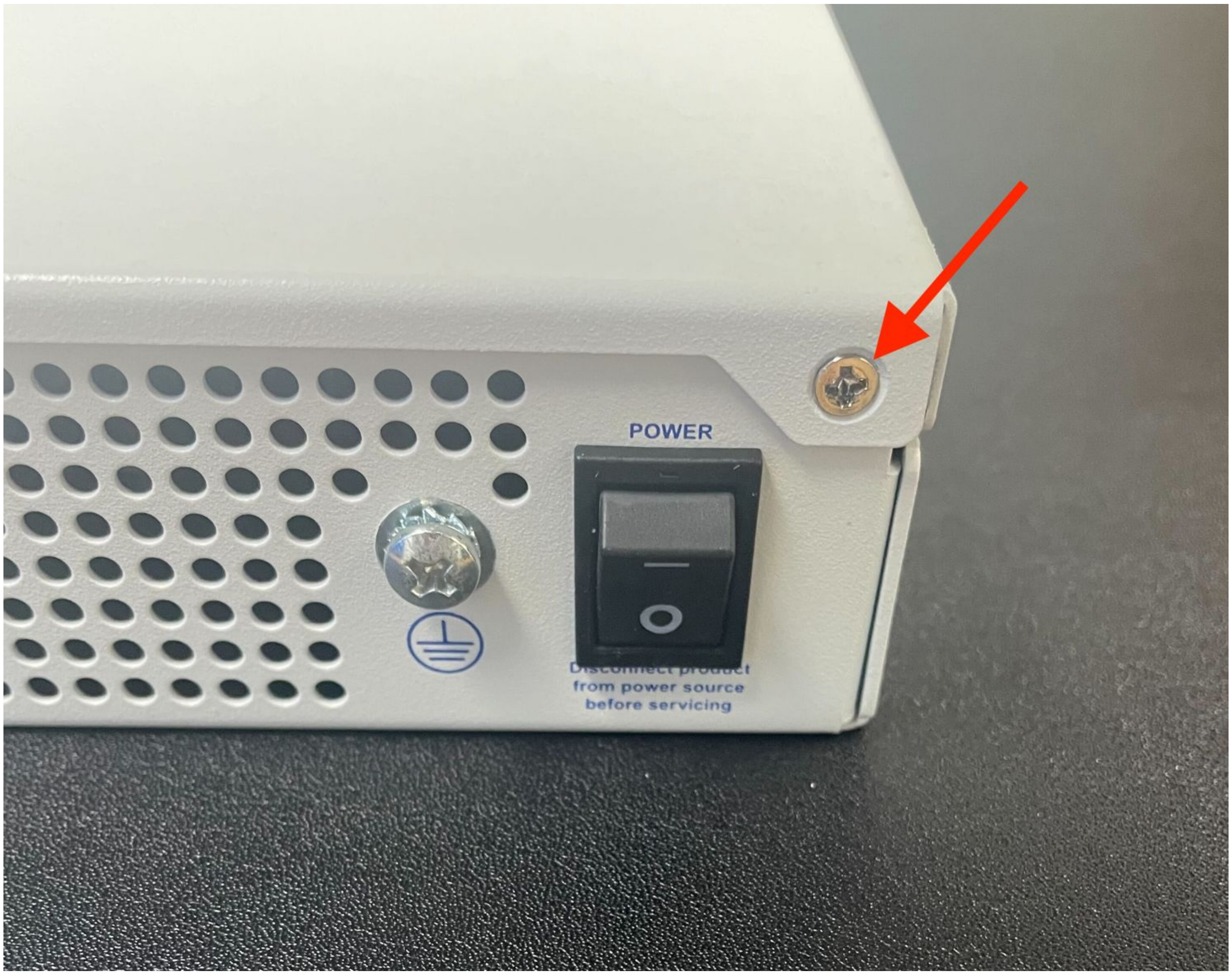


Fig. 5: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

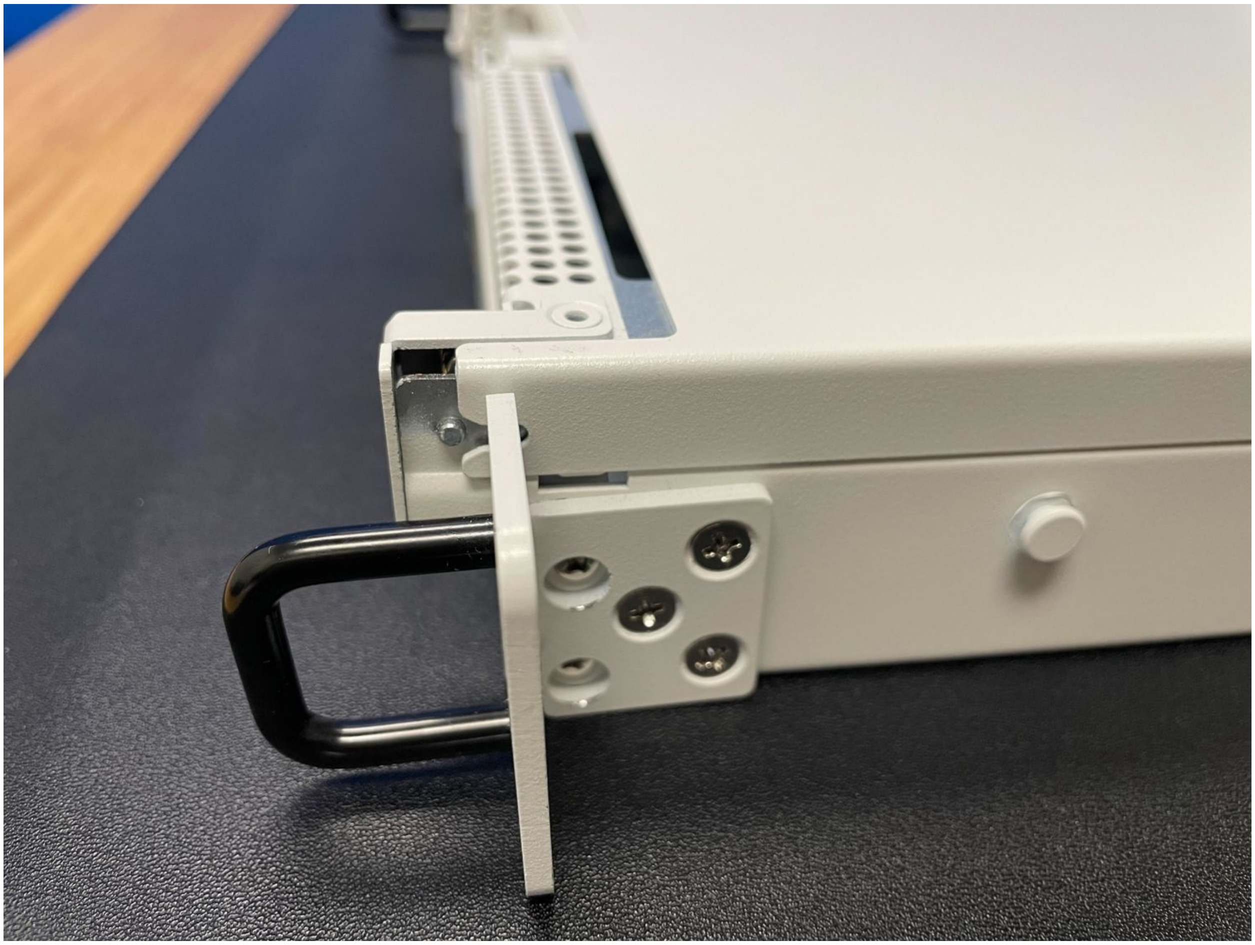


Fig. 6: Sliding back the top cover away from the front panel

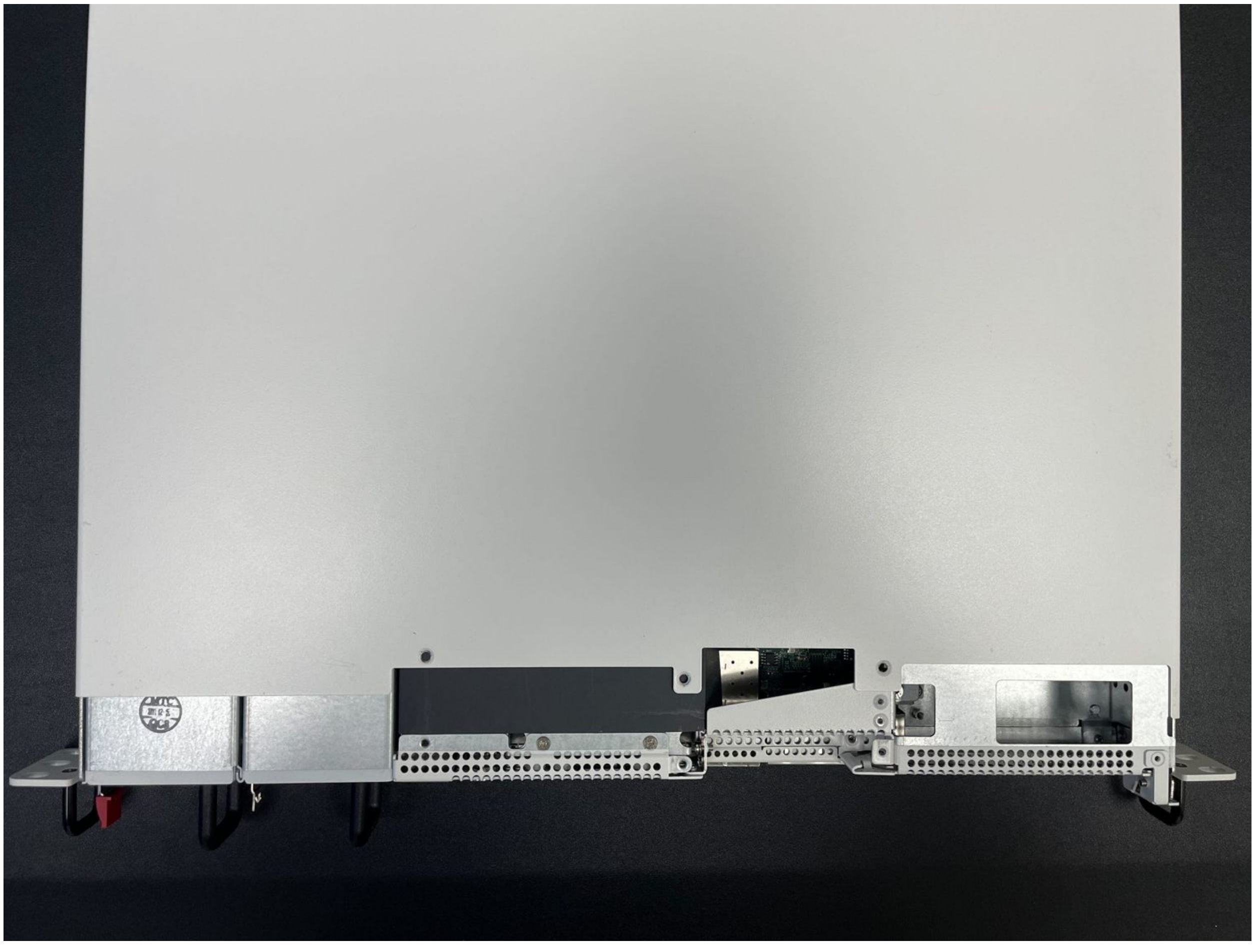


Fig. 7: Top cover in position to be lifted off

Note: These screws are captive and will not fully remove from the riser assembly. It is sufficient to loosen the screws until they no longer attach the riser assembly to the motherboard. This may be felt as a soft "click" when the screw is freely rotating and the threads are not engaged.

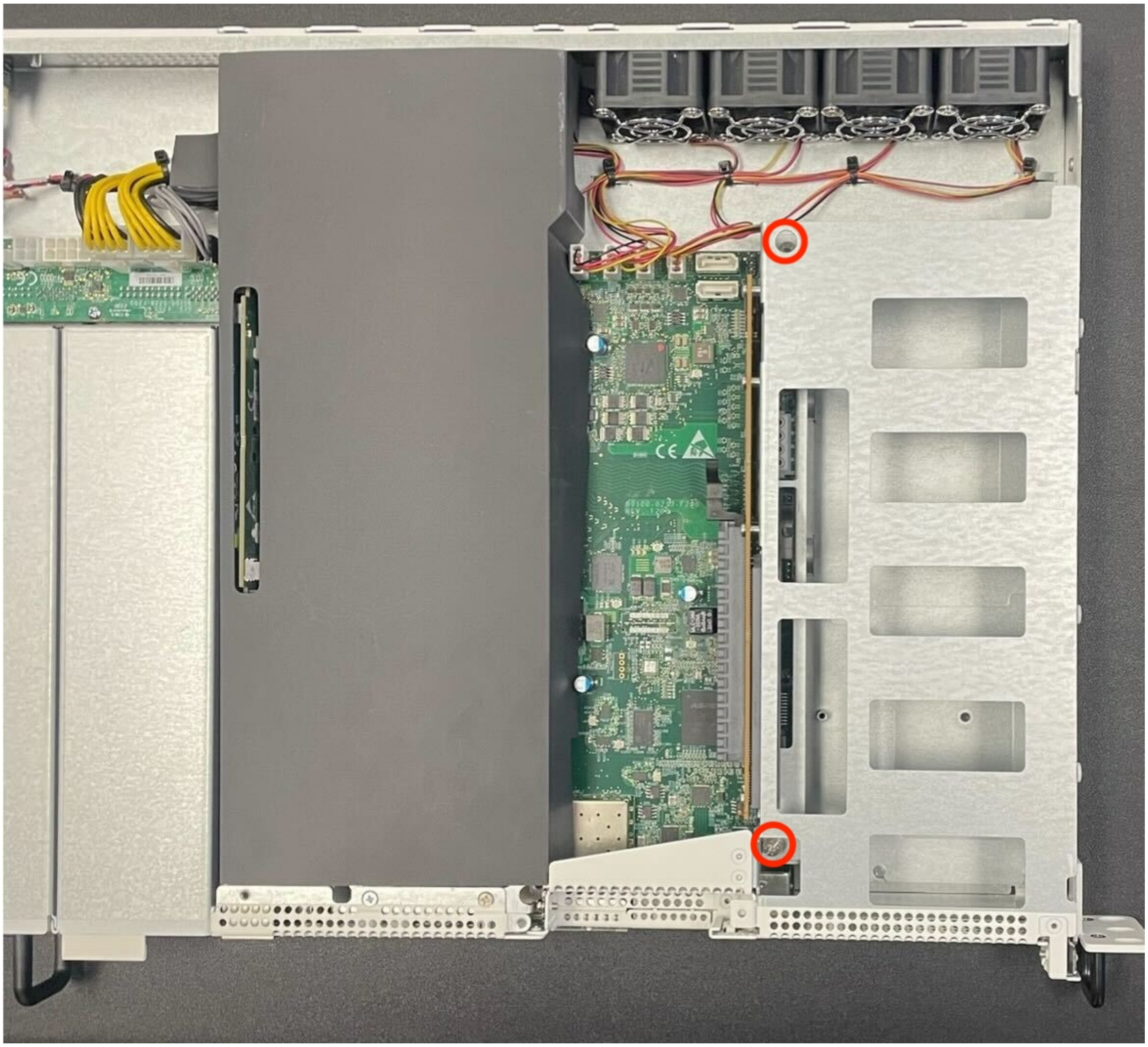


Fig. 8: Location of the captive riser assembly retaining screws indicated with red circles

2. Remove the riser assembly retaining screw on the front of the unit using the Phillips head screwdriver.
3. Carefully lift the riser assembly from the motherboard slot and remove the riser assembly.

   Rotating the assembly as seen in figures below can help the removal process with PCIe cards installed.

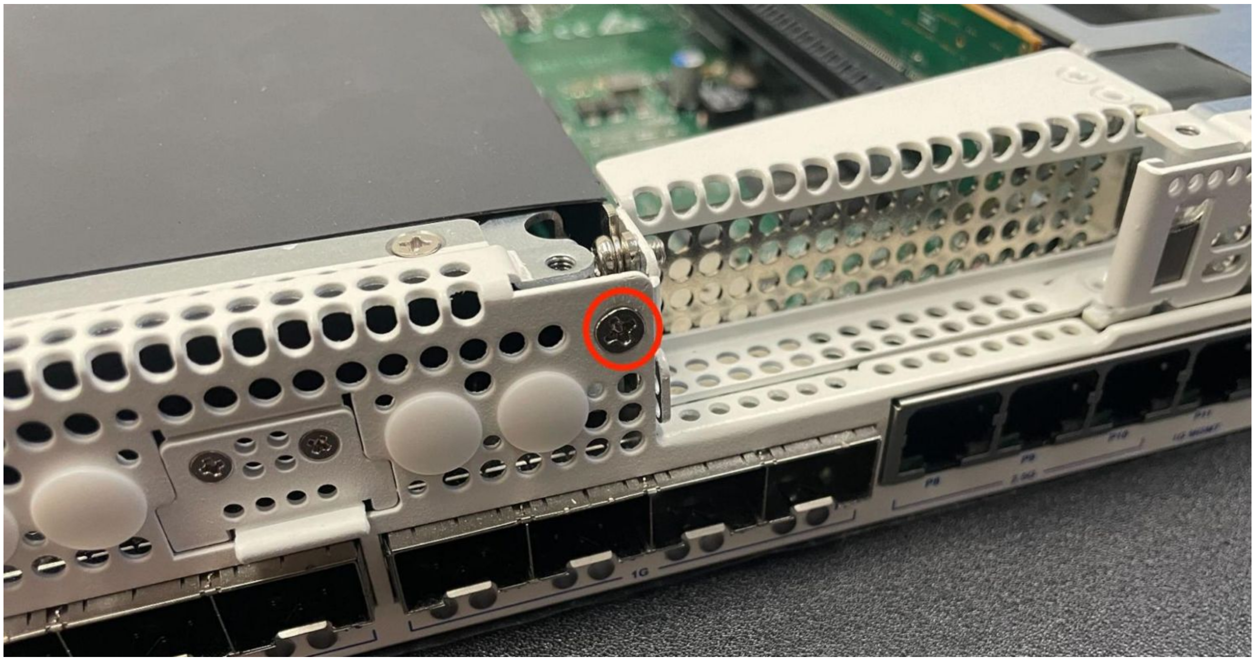


Fig. 9: Location of the riser assembly retaining screw on the front of the unit indicated with a red circle

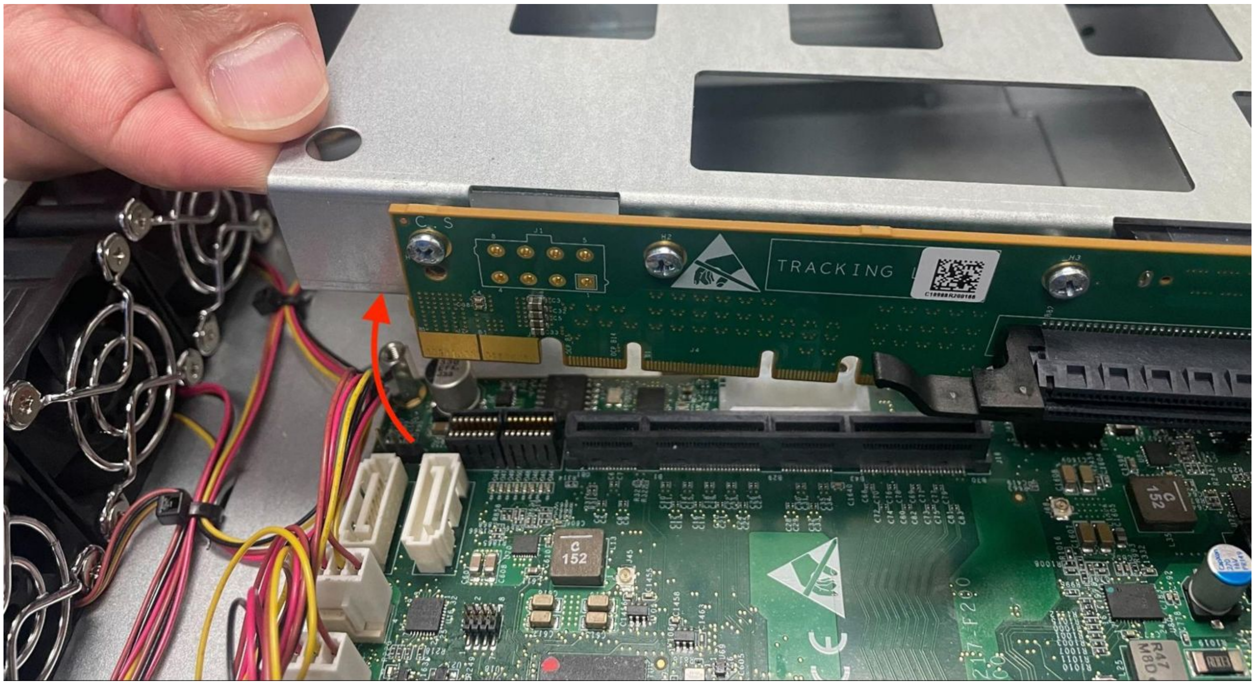


Fig. 10: Lift the riser assembly from the rear to remove it from the riser slot on the motherboard

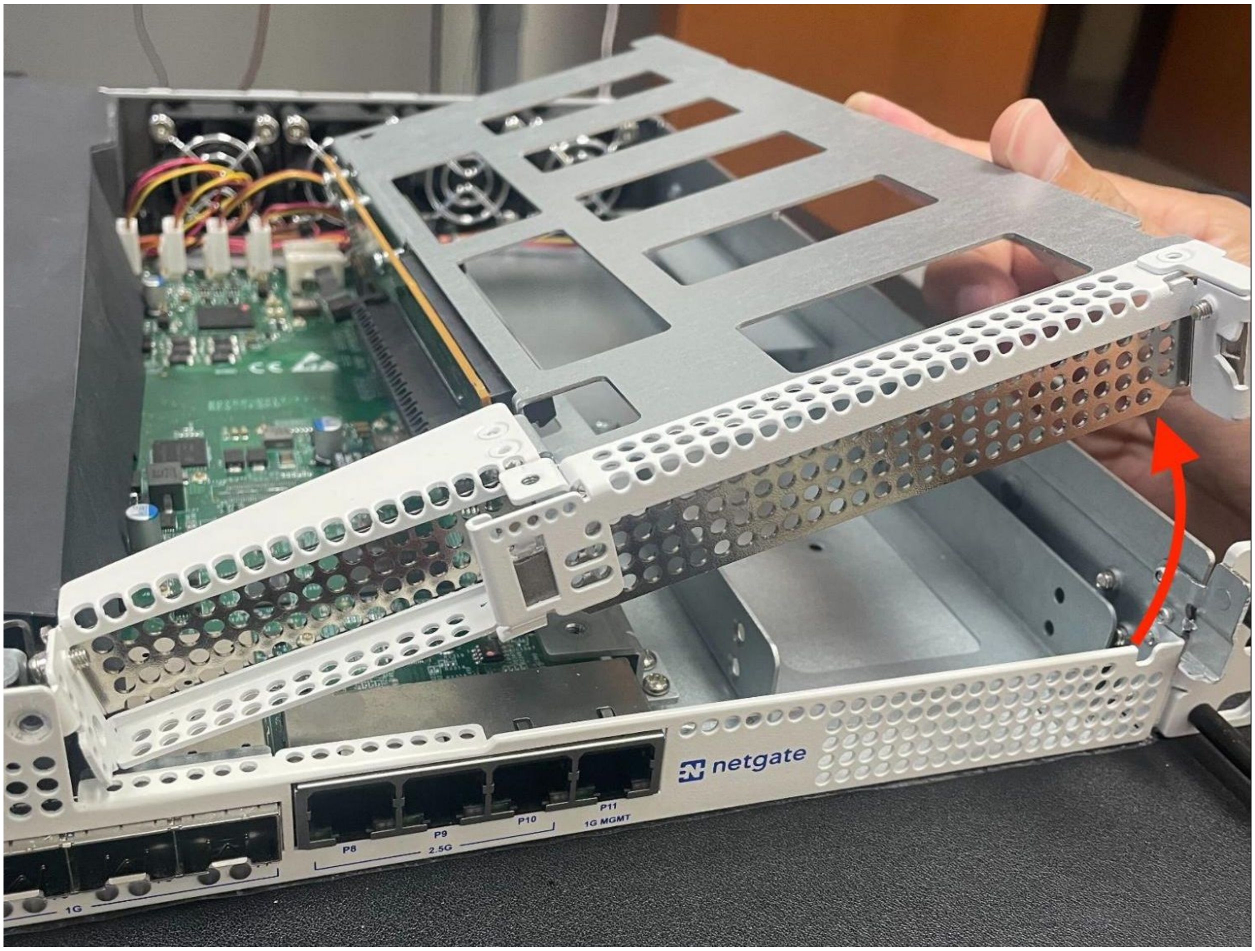


Fig. 11: Lift and rotate the riser assembly from the front as indicated by the red arrow to remove it from the chassis

8.3.5 Install the Add-on Expansion Card

With the riser assembly removed, it is time to install the add-on expansion card.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Locate the appropriate slot for the expansion card

   The expansion slot will vary depending on the card. For example, a card with a low profile bracket would most likely go in the smaller slot on the left, assuming its specifications match the slot capabilities. Some cards have alternate brackets so in those cases it is best to match the card based on its bus requirements, speed, and so on. See *Input and Output Ports* for the expansion slot specifications.

2. Loosen or remove the retaining screw from the expansion slot

   Tip: It is not typically necessary to fully remove the screw as the card can be moved around it when it is loosened, but removing the screw can make installing or removing the cards easier.

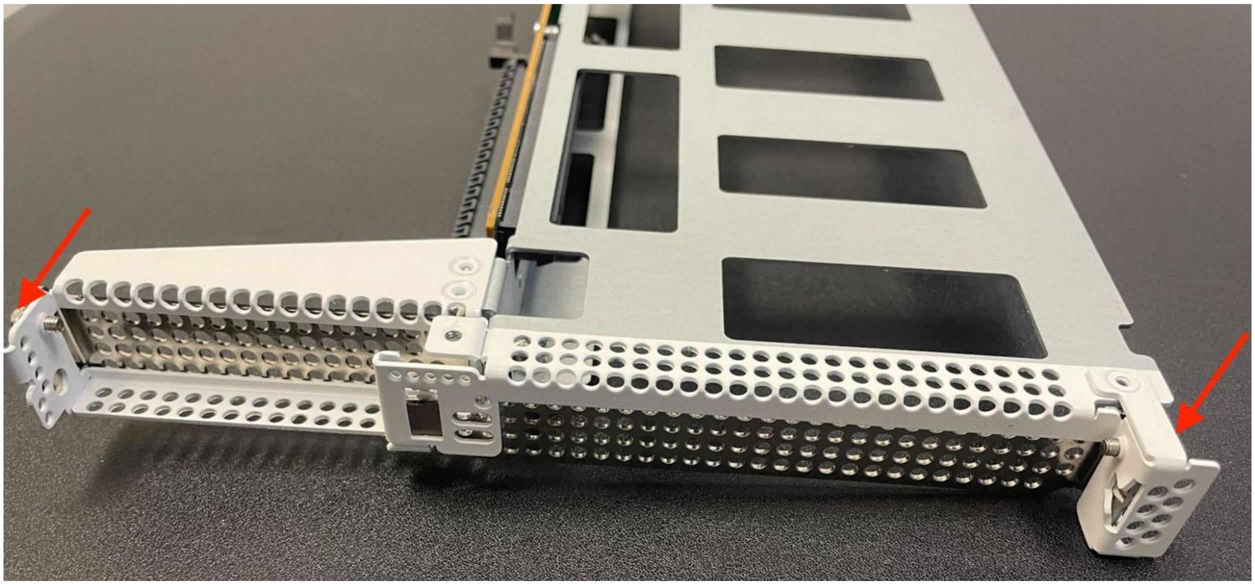


Fig. 12: Location of the add-on expansion card slot retaining screws indicated with red arrows

3. Remove the expansion slot cover by sliding it away from the center of the riser assembly and lifting it out, then set it aside.

   Note: The cover will not be necessary so long as there is a card in the expansion slot. Store the cover in a safe place in case it is needed in the future.

4. Install the add-on card into the expansion card slot by sliding it toward the center of the riser assembly until it is fully seated in its socket.

5. Ensure the card is properly aligned and fully inserted into the expansion card slot.

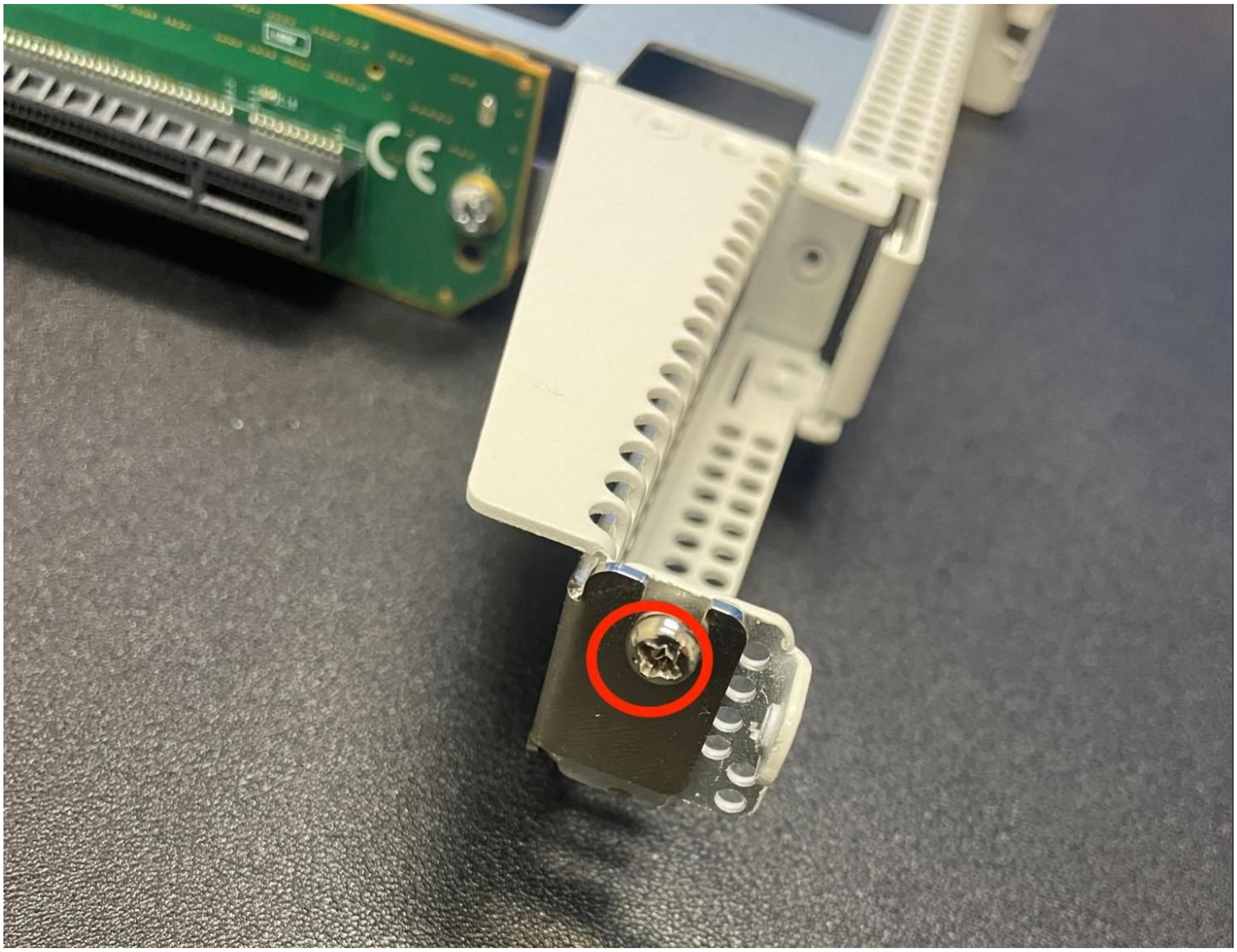


Fig. 13: Location of the low profile add-on expansion card slot retaining screw indicated with a red circle

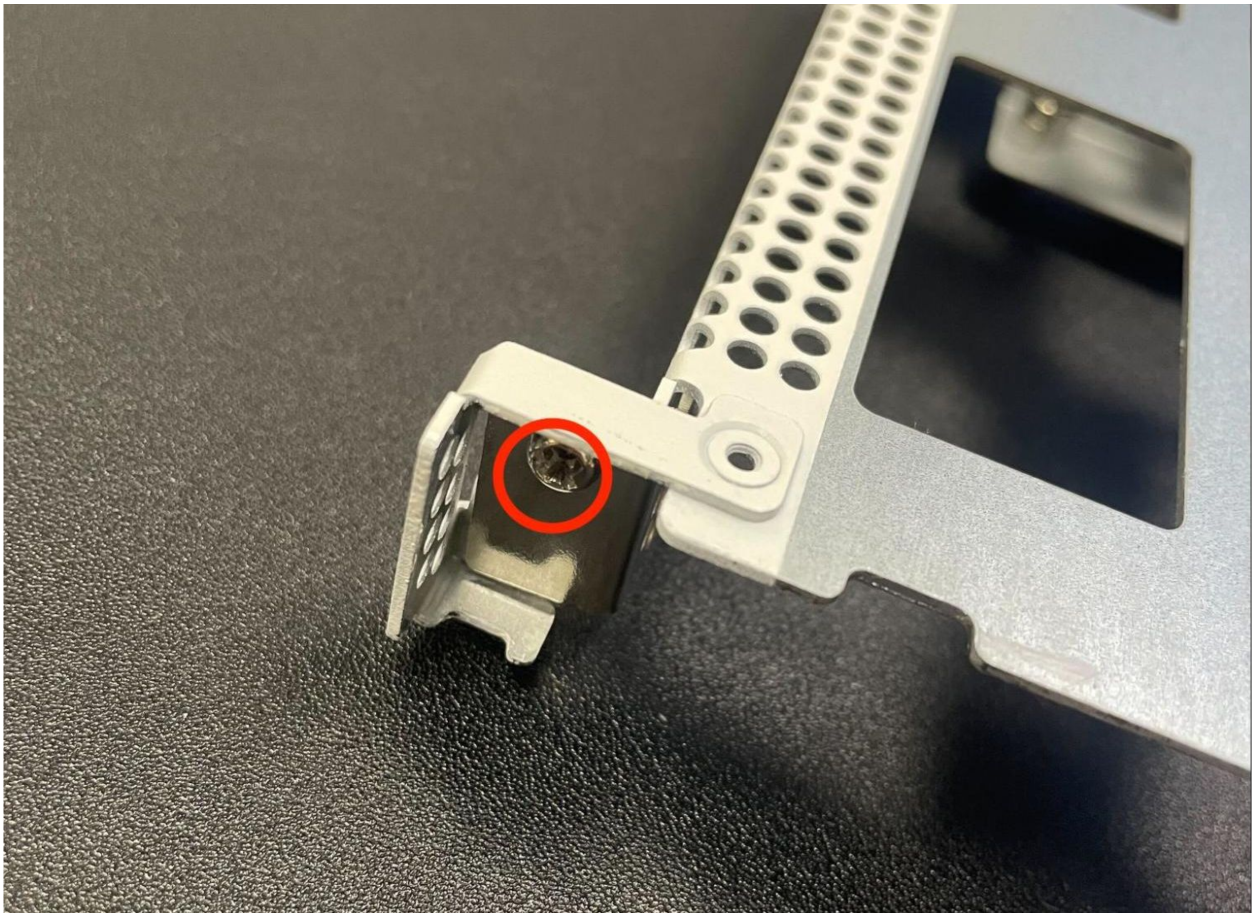


Fig. 14: Location of the full height add-on expansion card slot retaining screw indicated with a red circle

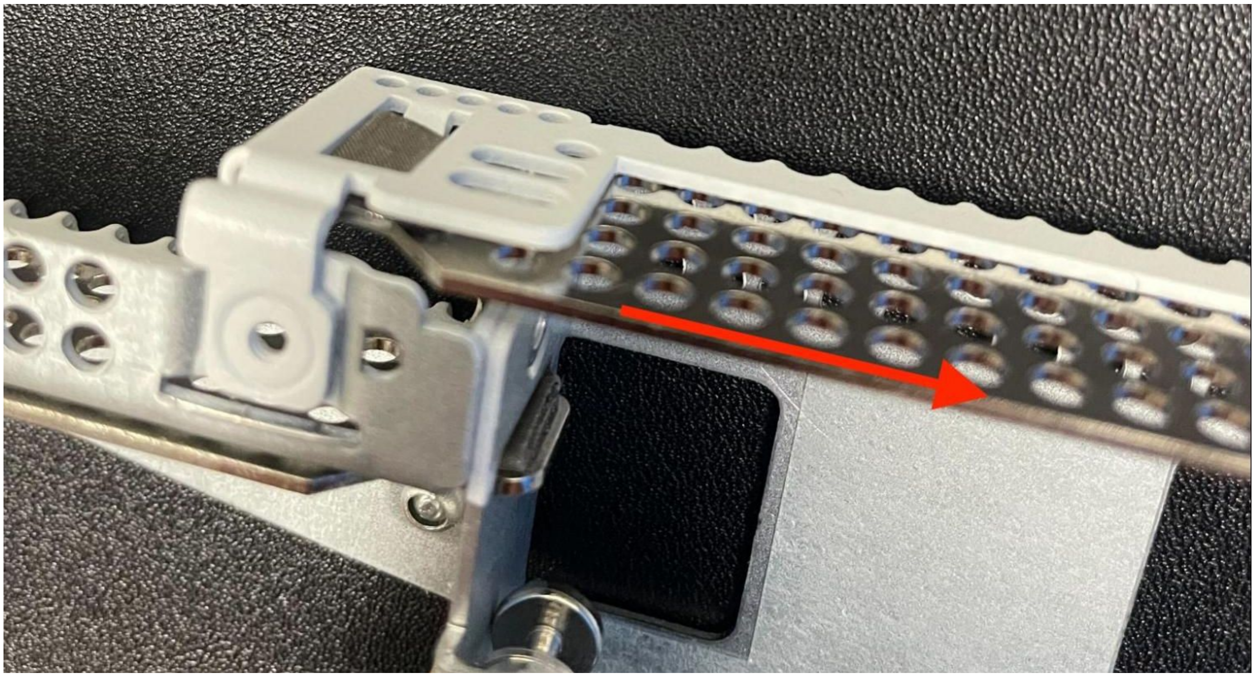


Fig. 15: Slide the expansion slot cover away from the center of the riser assembly

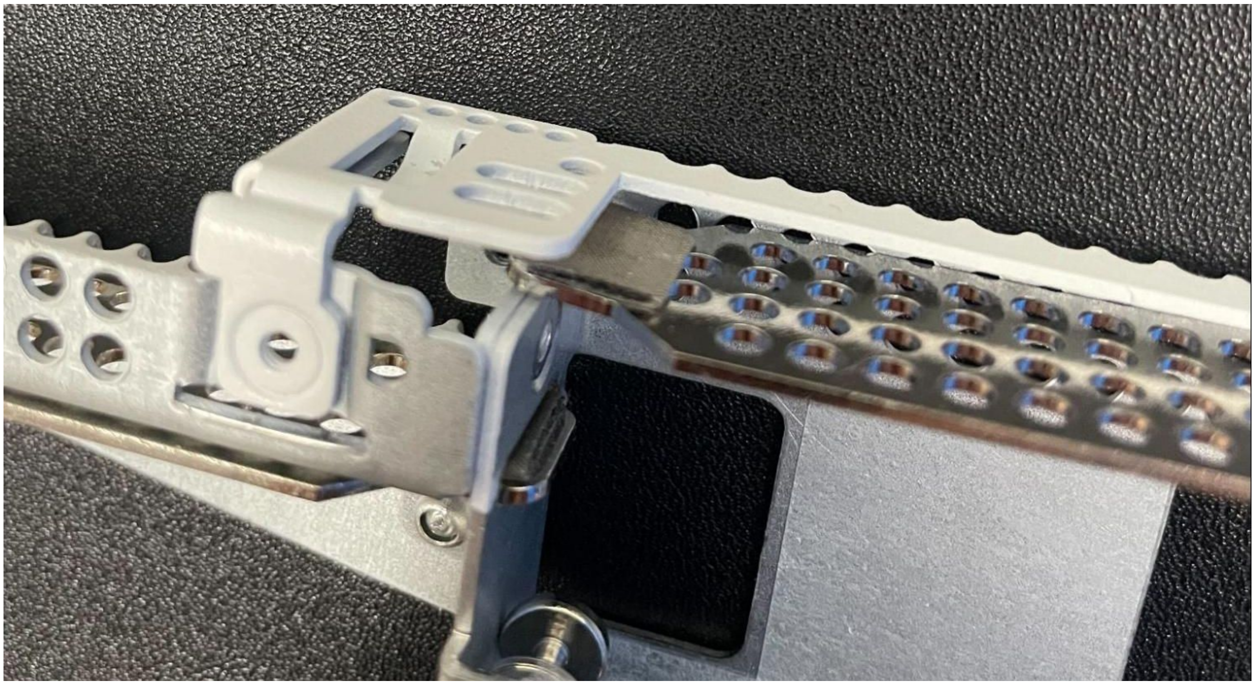


Fig. 16: Remove the expansion slot cover once it is free from the expansion slot

The rear of the socket has a retention clip to hold the card in place which should be engaged once the card is fully seated

The front of the card should be flush with the front of the riser assembly and aligned with the retention screw hole.

6. Fasten the expansion card to the riser assembly using the retaining screw and the Phillips head screwdriver.

8.3.6 Replace the Riser Assembly

With the expansion card installed in the riser assembly, replace the riser assembly back into the chassis.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Insert the riser card back into the chassis and fully seat it into the slot on the motherboard.
2. Replace the riser assembly retaining screw on the front of the unit using the Phillips head screwdriver.
3. Tighten the two captive screws which attach the riser assembly to the motherboard using the Phillips head screwdriver.

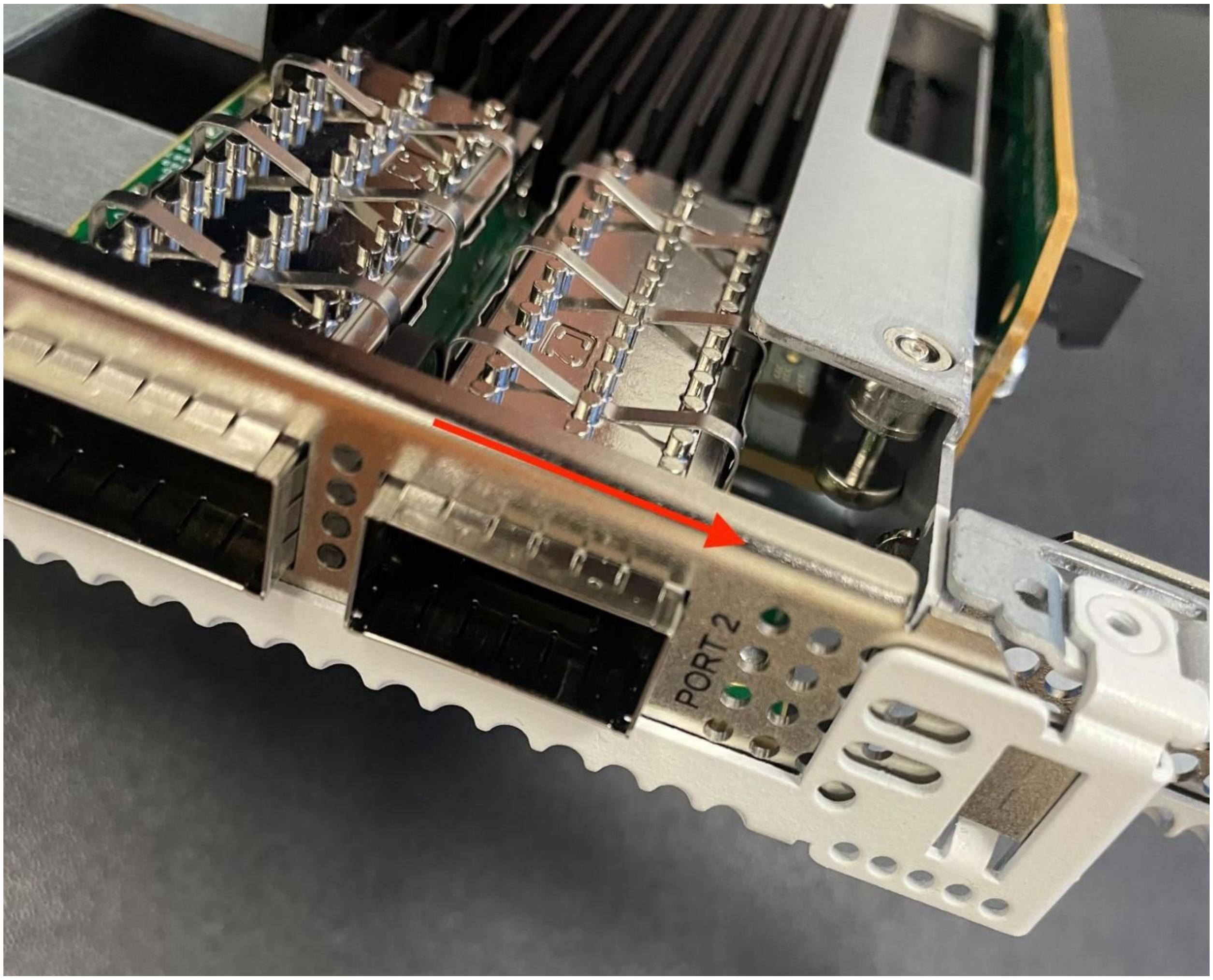


Fig. 17: Installing an add-on network interface card into an expansion slot

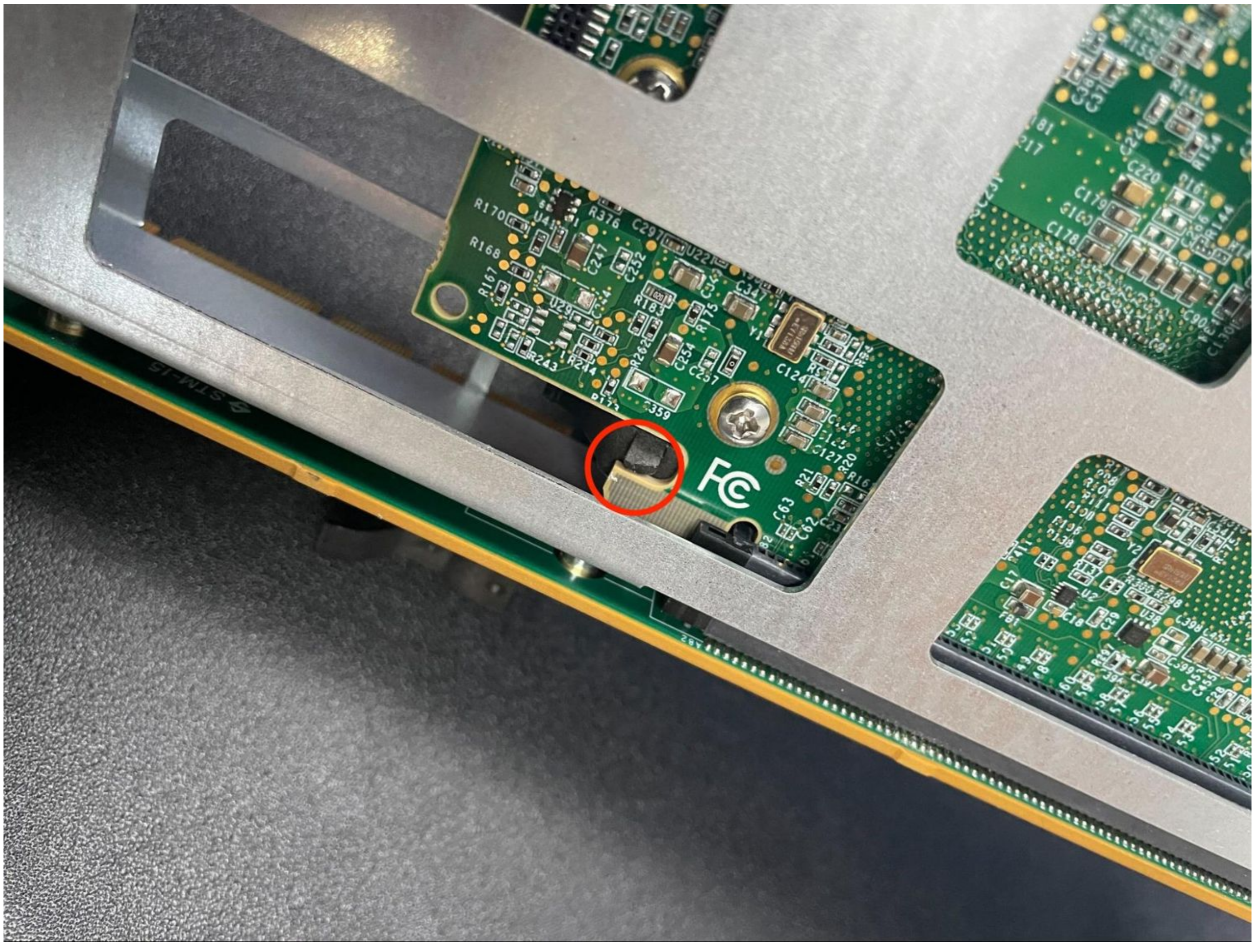


Fig. 18: Expansion card slot retention clip holding a card in place

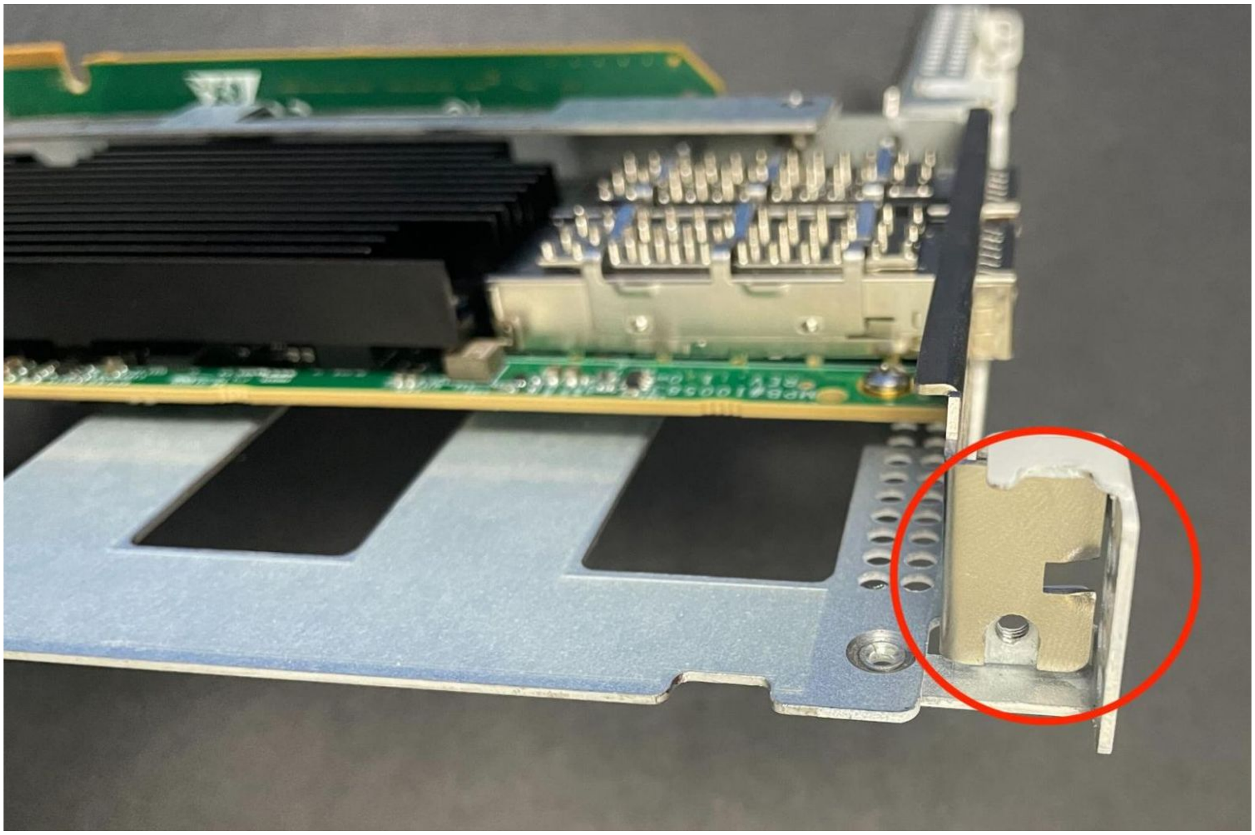


Fig. 19: Expansion card aligned with the riser assembly and retention screw hole

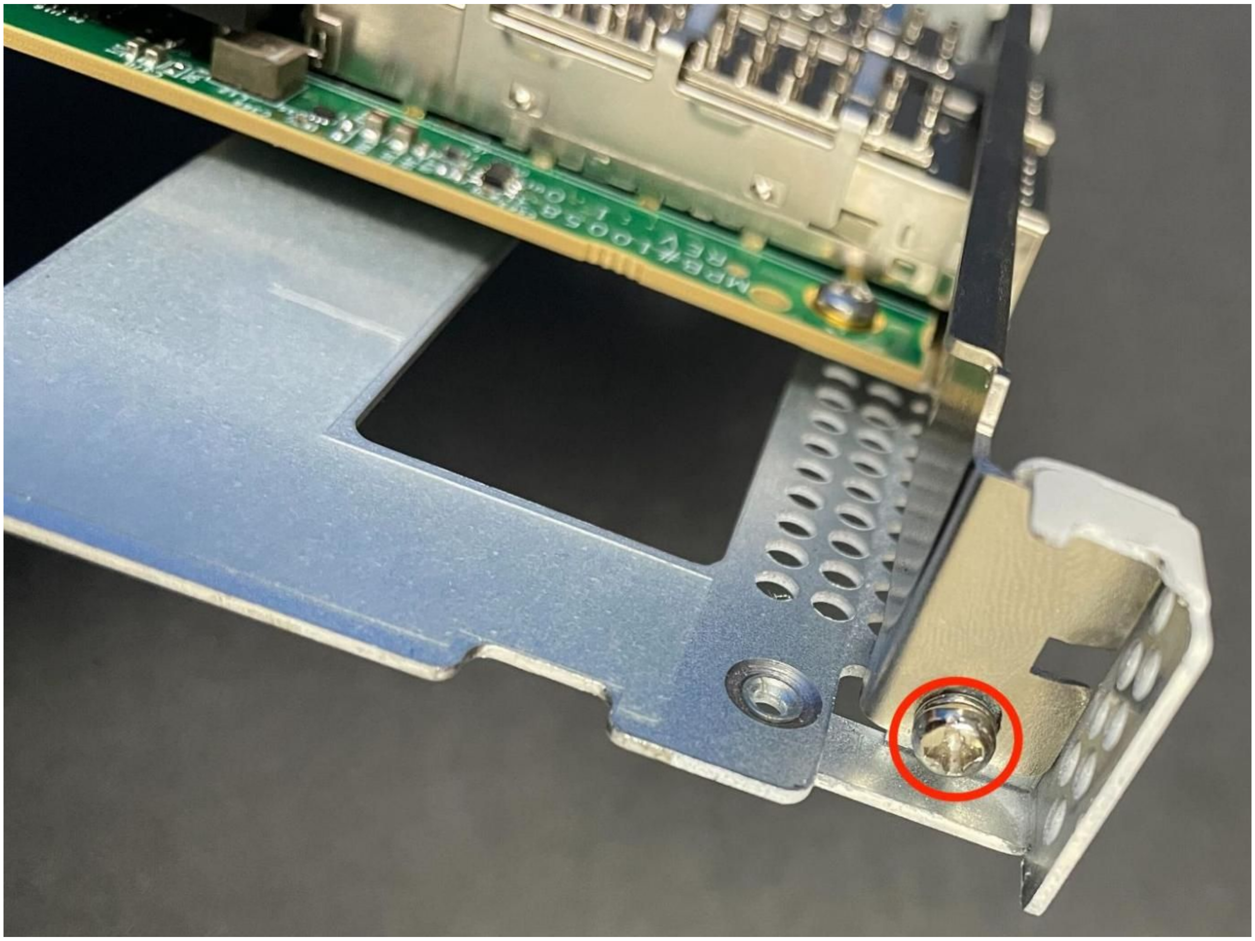


Fig. 20: Expansion card fastened in the riser assembly using the retention screw

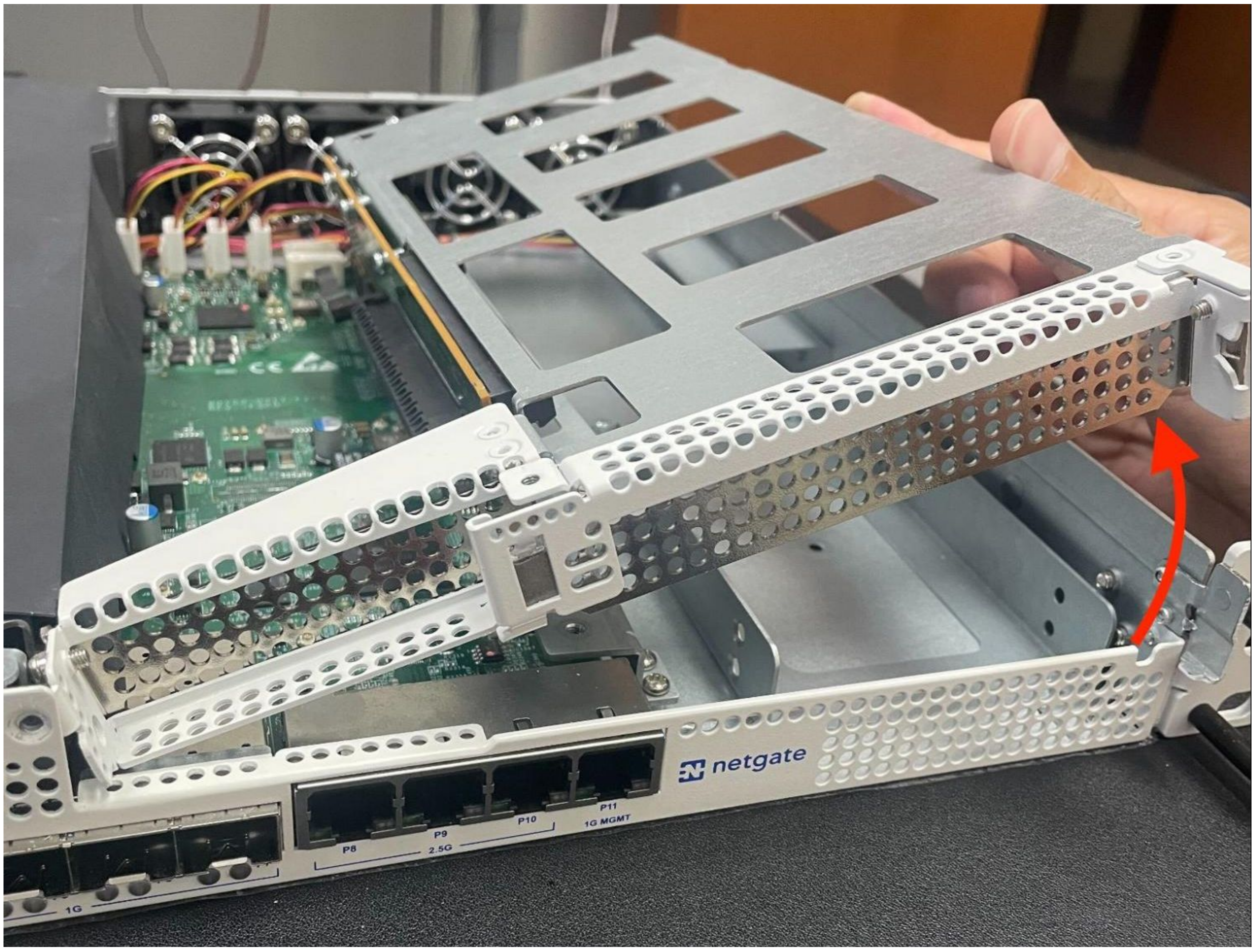


Fig. 21: Rotate and replace the riser assembly from the front in the **opposite** direction indicated by the red arrow

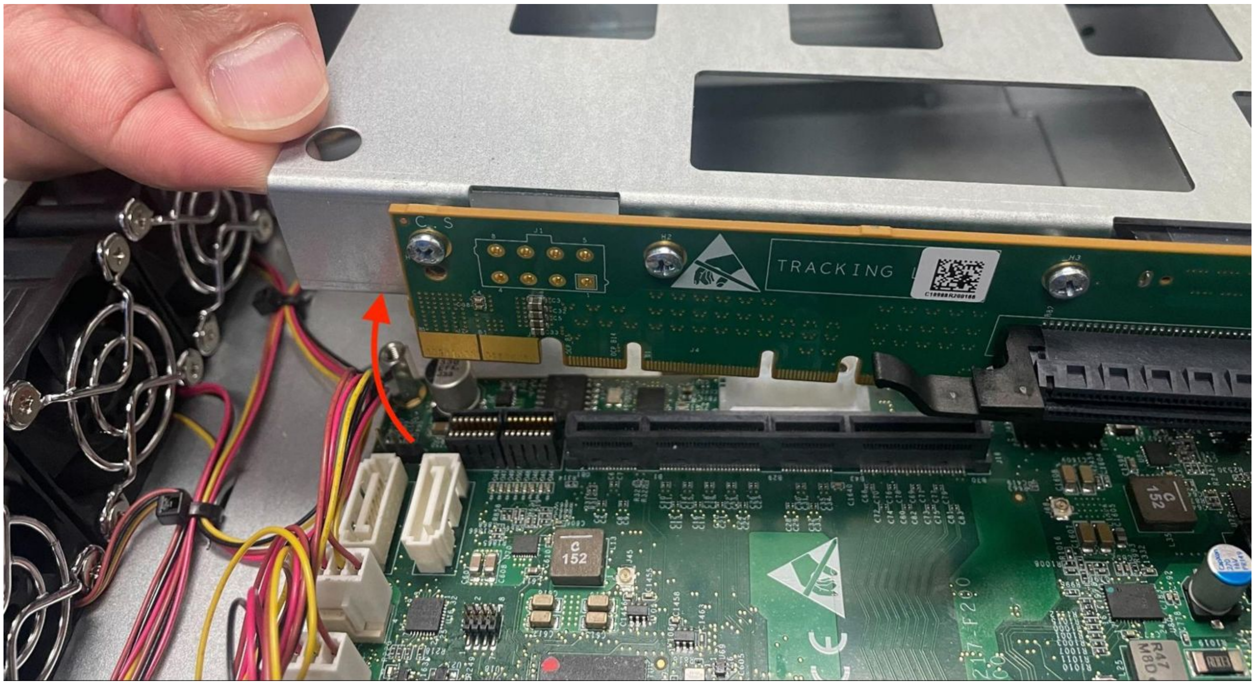


Fig. 22: Re-seat the riser assembly in the the riser slot from the rear of the motherboard in the **opposite** of the direction indicated by the red arrow

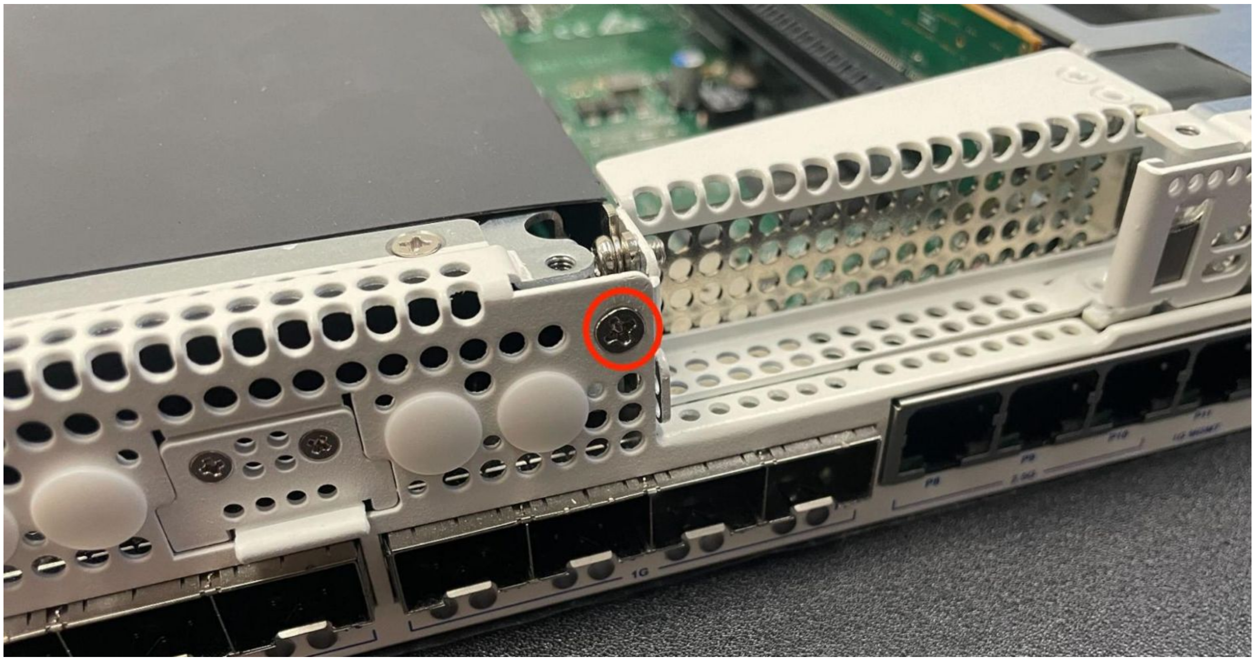


Fig. 23: Location of the riser assembly retaining screw on the front of the unit indicated with a red circle

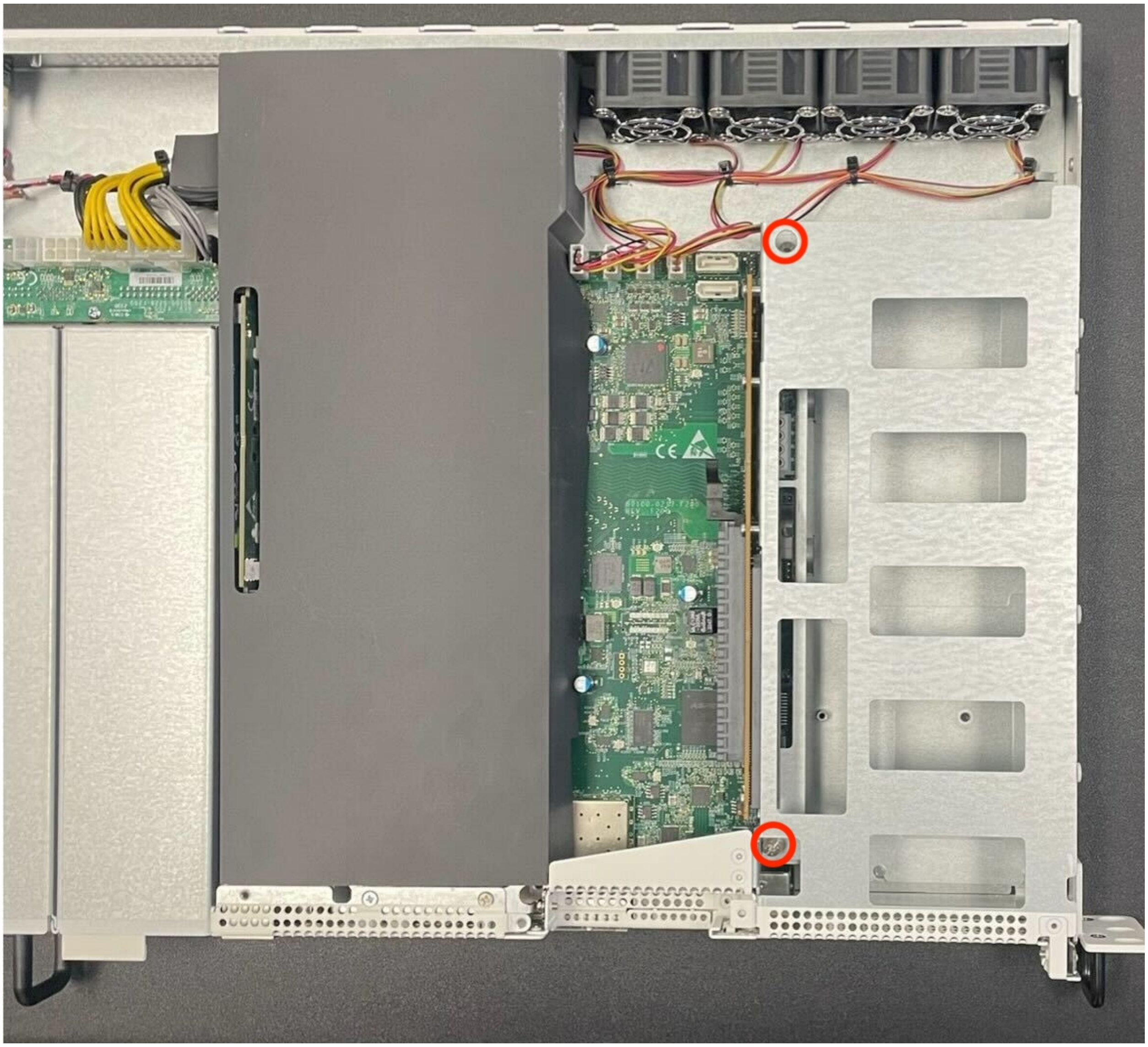


Fig. 24: Location of the captive riser assembly retaining screws indicated with red circles

8.3.7 Replacing and Fastening the Lid

With the internal components all in place, the next step is to replace the lid and all its fasteners.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.
- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Align the top cover with the top of the unit, a short distance behind the front panel.

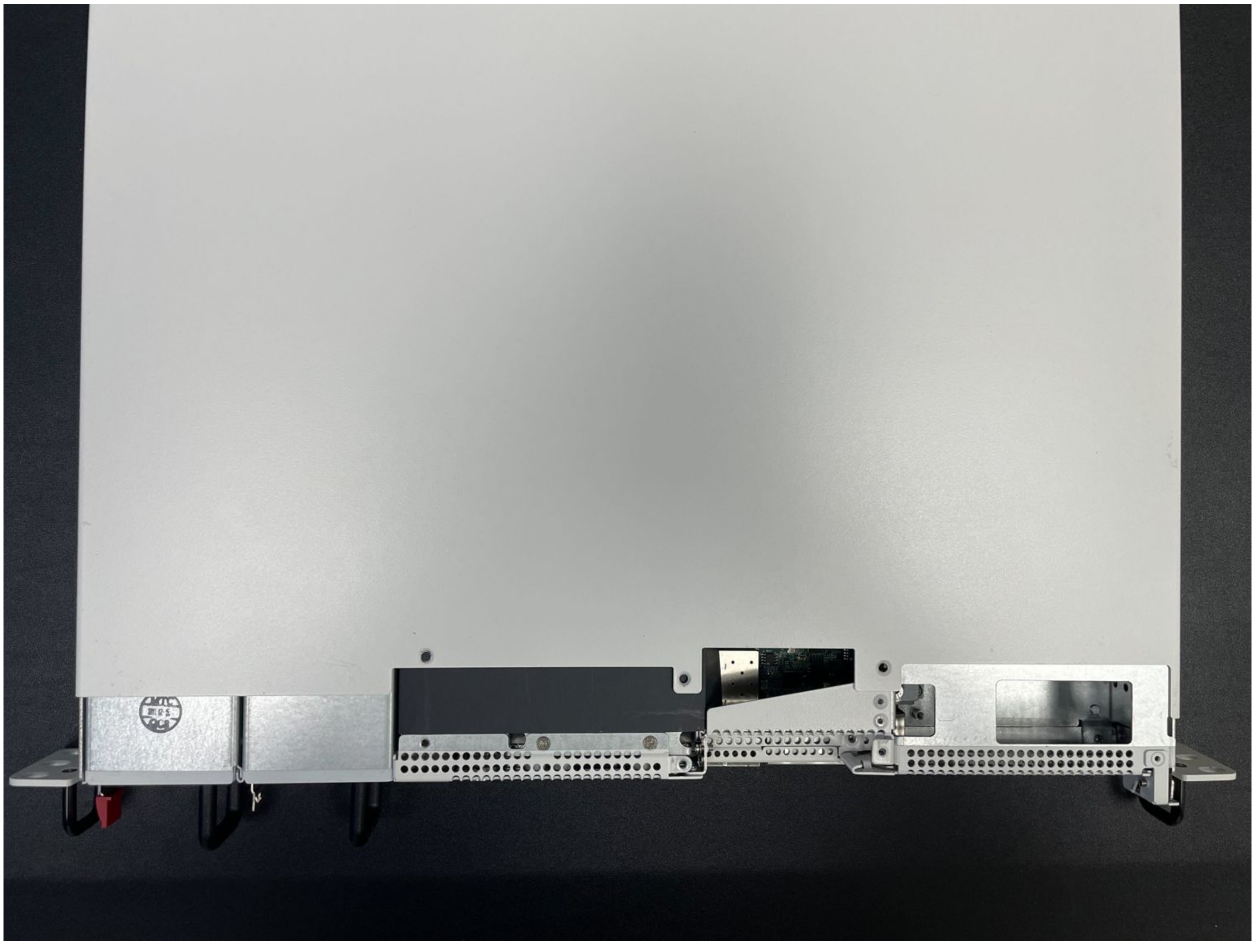


Fig. 25: Top cover in position to be replaced

2. Slide the top cover toward the front of the unit into its closed position.

# Replace the screws on the rear of the unit (left and right top corners) using
the Phillips head screwdriver.

# Replace the screws on the top of the unit using the Phillips head screwdriver.

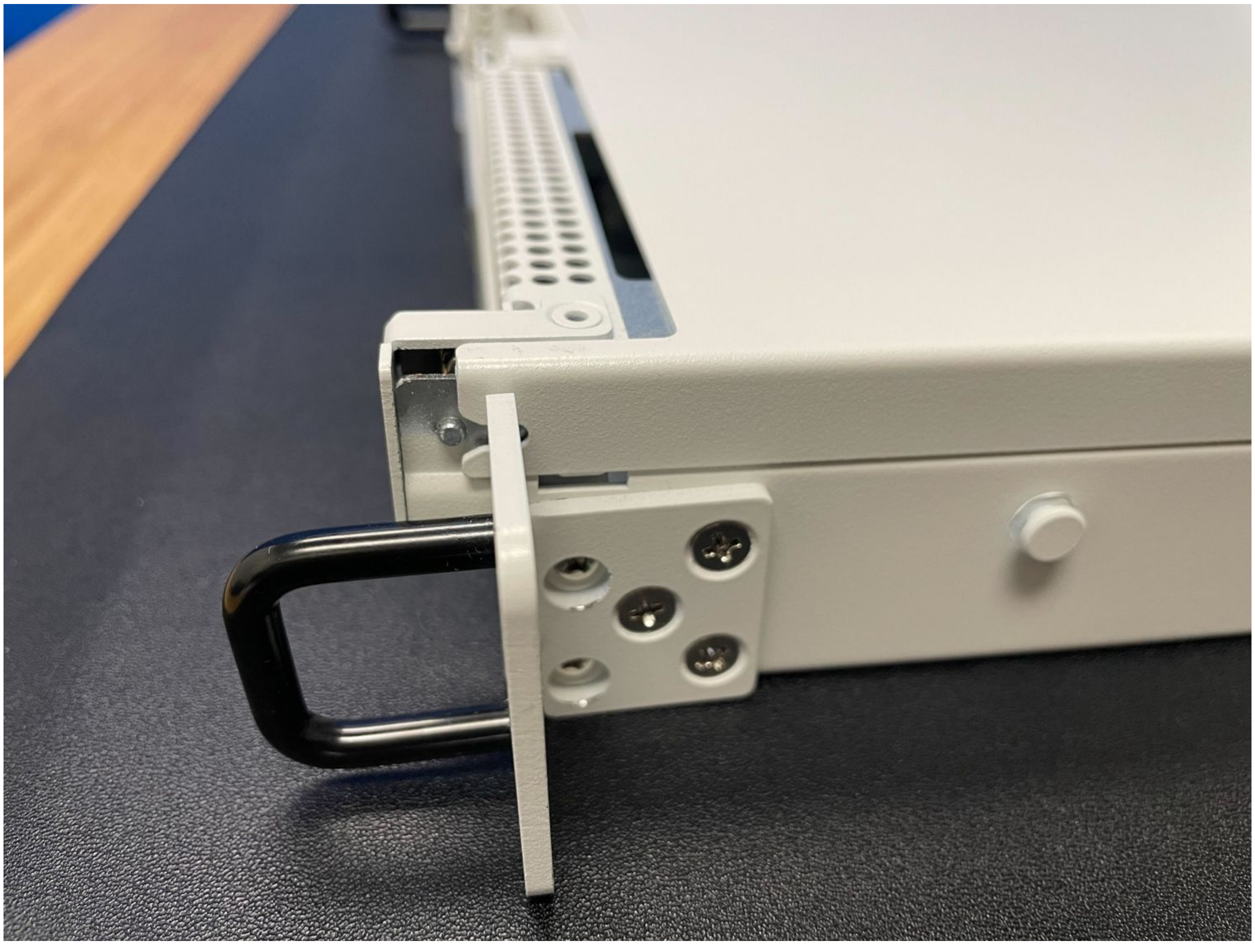


Fig. 26: Slide the top cover back toward the front panel

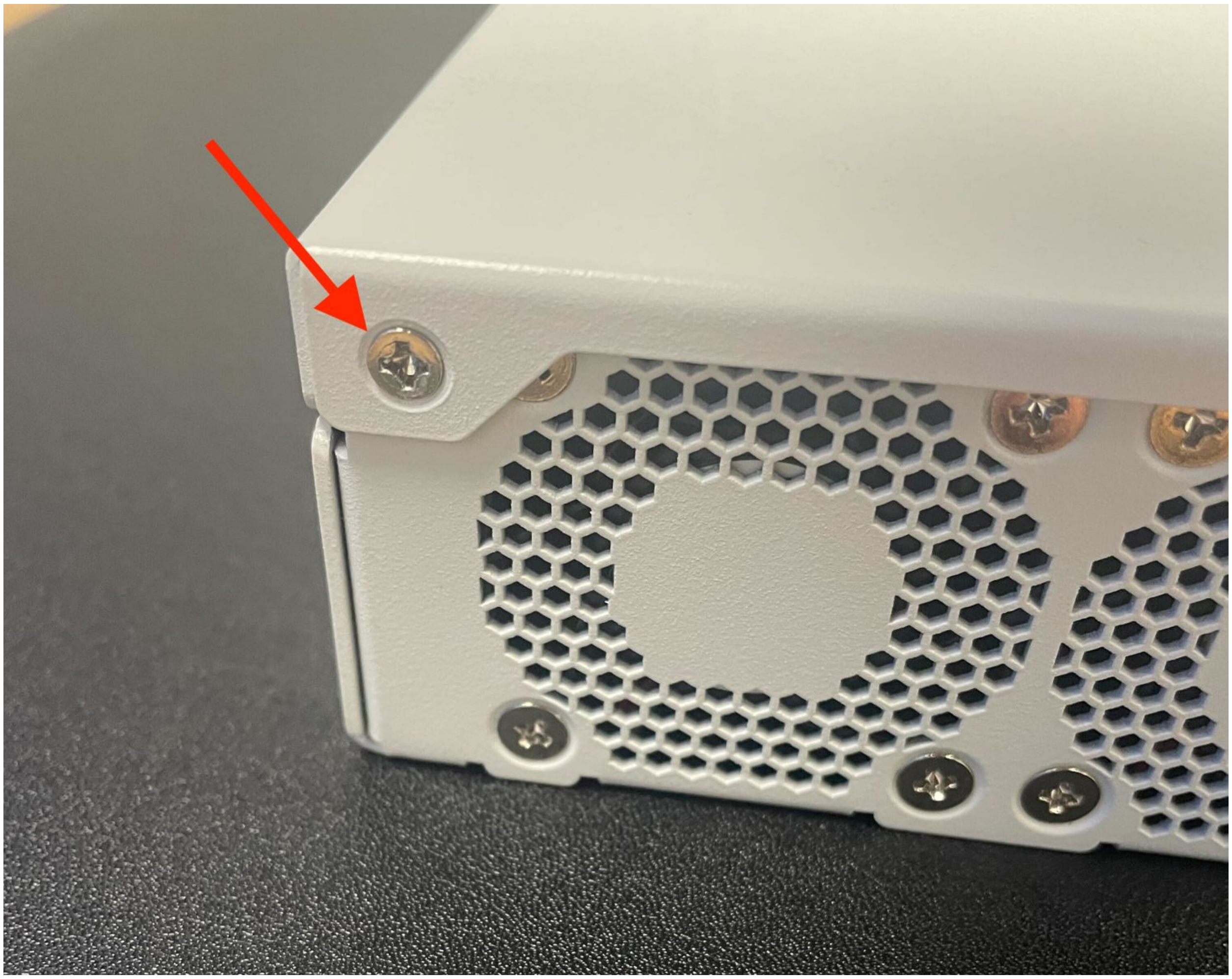


Fig. 27: Screw on the rear side of the unit at the left top corner, indicated with an arrow.

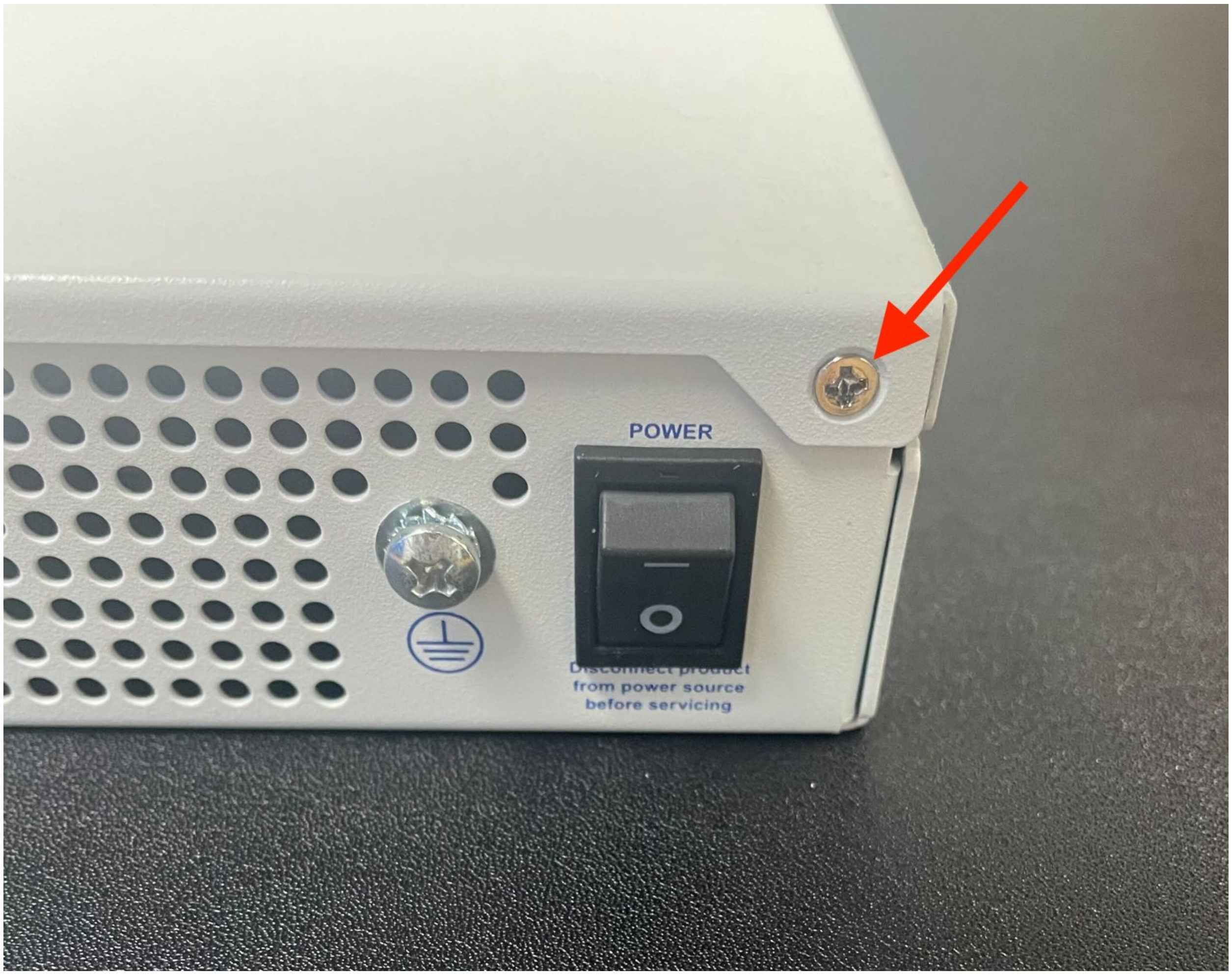


Fig. 28: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

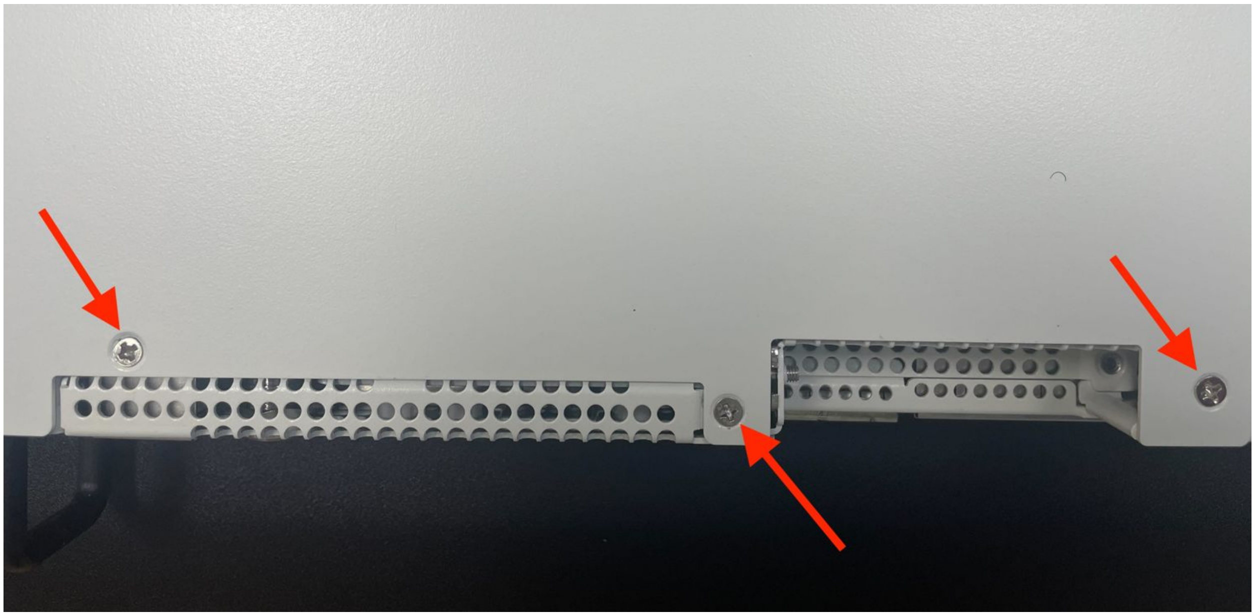


Fig. 29: Screws on the top of the cover at the front of the unit, indicated with arrows

8.3.8 Reconnect

The device is now ready to be put back into its former location.

1. Mount the Netgate 8300 in the rack
2. Plug in all network cables, USB cables and devices, serial console connections, etc.
3. Insert the USB memstick containing the installation media
4. Plug the power cables into all installed power supply units.
5. Turn power on to the unit by changing the power switch on the rear of the unit to the **on** position.
6. Reconnect to the serial console

8.3.9 Enable Interfaces (Network Interface Cards Only)

If the expansion card added to the device is a network interface card, this must be accounted for in TNSR software once the card is in place.

The interfaces can be enabled for use in the dataplane as needed based on the information in the TNSR software documentation for dataplane interfaces.

See also:

See *Networking Ports* for more information.

See also:

Netgate TAC may be able to assist with adjusting configurations for customers in many cases.

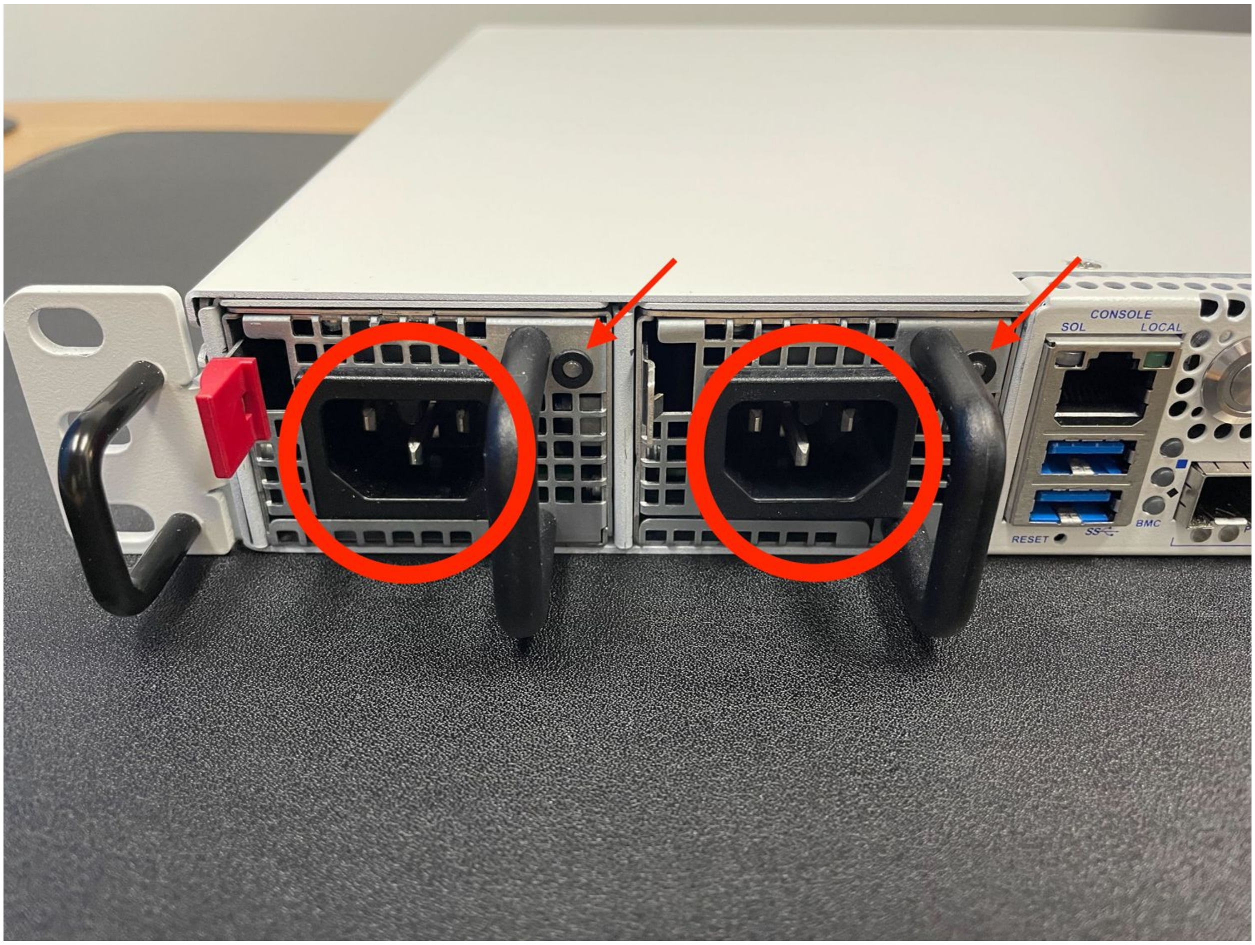


Fig. 30: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

8.3.10 Re-arm the Intrusion Sensor

Opening the case to install the expansion card will trigger the intrusion alarm sensor, even while the device is removed from power. The intrusion alarm causes the fans to run at a higher fixed speed until the sensor is re-armed.

Once TNSR software is up and running, follow the procedure in *Re-arm the Chassis Intrusion Switch* to reset the sensor.

CHAPTER

NINE

ADDITIONAL RESOURCES

9.1 Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

https://www.netgate.com/our-services/professional-services.html

9.2 Netgate Training

Netgate training offers training courses for increasing your knowledge of Netgate products and services. Whether you need to maintain or improve the security skills of your staff or offer highly specialized support and improve your customer satisfaction; Netgate training has got you covered.

https://www.netgate.com/training/

9.3 Resource Library

To learn more about how to use your Netgate appliance and for other helpful resources, make sure to browse our Resource Library.

https://www.netgate.com/resources/

CHAPTER

TEN

WARRANTY AND SUPPORT

- One year manufacturer's warranty.
- Please contact Netgate for warranty information or view the Product Lifecycle page.
- All Specifications subject to change without notice.

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

For more information on how to use TNSR® software, see the TNSR Documentation and Resource Library.