Upgrade and Downgrade Process

Table of contents

The following pages provide information on upgrading and downgrading the operating system version on the device.

- Important Pre-OS Upgrade Notes
- Upgrading Operating System Software
- Upgrading HA Groups
- Upgrading MLNX-OS Software on Modular Switches
- Deleting Unused Images
- Downgrading OS Software
- Upgrading System Firmware
- Software Management Commands

Important Pre-OS Upgrade Notes

Please consider the following items prior to upgrading the operating system:

- Upgrading modular switch systems can take up to 30 minutes during which time the system is indisposed
- Upgrading the OS while embedded SM is enabled may cause the command “no hostname” to fail upon first execution. To resolve this, rerun the command
- The upgrade procedure burns the software image as well as the firmware should there be a need
- Before upgrading the software image on your system, make sure to close all CLI sessions besides the one used to run the upgrade process
- If running a system with dual management cards, refer to “Upgrading MLNX-OS Software on Modular Switches”
- To upgrade the MLNX-OS version on an SM cluster, please refer to “Upgrading HA Groups”
- The End-User License Agreement (EULA) must read and accepted after image upgrade in case the EULA is modified. The EULA link is only available upon first login to CLI
- Linux docker container names are limited to 180 characters. Upgrading to this version removes containers which do not comply with this limitation and prints the following warning to the log: “Removed configuration of container: <container name>, container name is limited to 180 characters”

Upgrading Operating System Software

To upgrade MLNX-OS, perform the following steps.

1. Enter Config mode.

```
switch > enable
switch # configure terminal
switch (config) #
```

2. Display the currently available image (.img file).

```
switch (config) # show images
Installed images:

  Partition 1:
  <old_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <old_image>
```

```
Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

3. Delete the image listed under “Images available to be installed” prior to fetching the new image. Use the command “image delete” for this purpose.

```
switch (config) # image delete <old_image>
```

> **Note**
>
> When deleting an image, it is recommended to delete the file, but not the partition, so as to not overload system resources.

4. Fetch the new software image.

```
switch (config) # image fetch scp://<username>:<password>@<ip-address>/var/www/html/<new_image>
Password (if required): ****** 100.0%
[##########################################################
```

5. Display the available images again and verify that the new image now appears under “Images available to be installed”.

> **Note**
>
> To recover from image corruption (e.g., due to power interruption), there are two installed images on the system. See the commands “image boot next” and “image boot location” for more information.

```
switch (config) # show images
Installed images:

  Partition 1:
  <old_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <new_image>

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
```

```
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

6. Install the new image.

```
switch (config) # image install <new_image>
Step 1 of 4: Verify Image
 100.0%
[############################################################
Step 2 of 4: Uncompress Image
 100.0%
[############################################################
Step 3 of 4: Create Filesystems
 100.0%
[############################################################
Step 4 of 4: Extract Image
 100.0%
[############################################################
```

> **Note**
>
> CPU utilization may go up to 100% during image upgrade.

7. Have the new image activate during the next boot.

```
switch (config) # image boot next
```

8. Run “show images” to review your images.

```
switch (config) # show images
Installed images:

  Partition 1:
  <new_image>

  Partition 2:
  <old_image>

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
 webimage.tbz
  <new_image>

Serve image files via HTTP/HTTPS: no

No image install currently in progress.

Boot manager password is set.

Image signing: trusted signature always required
Admin require signed images: yes

Settings for next boot only:
   Fallback reboot on configuration failure: yes (default)
```

9. Save current configuration.

```
switch (config) # configuration write
```

10. Reboot to run the new image.

```
switch (config) # reload
Configuration has been modified; save first? [yes] yes
Configuration changes saved.
Rebooting...
switch (config)#
```

Note

After software reboot, the software upgrade will also automatically upgrade the firmware version.

Note

On systems with dual management, the software must be upgraded on both the host and the device modules.

Note

In order to upgrade the system on dual management system, refer to "Upgrading MLNX-OS Software on Modular Switches".

Note

When performing an upgrade from the WebUI, make sure that the image being upgraded to is not already located in the system (i.e., fetched from the CLI).

Upgrading HA Groups

If fallback is ever necessary in an HA group, all cluster nodes must have the same OS version installed and they must be immediately reloaded.

To upgrade MLNX-OS version without affecting an HA group:

1. Identify the HA group master.

   For IB HA. Run:

```
switch (config) # show ib ha
Global HA state
==================
IB Subnet HA name:subnet4
HA IP address: 192.168.10.43/24
Active HA nodes: 2
ID              State Role          IP                  SM
Priority
-------------------------------------------------------------------
-------
switch          standalone          192.168.10.42       disabled
switch          master              192.168.10.18       disabled
```

2. Upgrade standby node in the HA group according to steps 1-10 in "Upgrading Operating System Software".

3. Wait until all standby nodes have rejoined the group.

> **Note**
>
> In situations of heavy CPU load or noisy network, it is possible that another node assumes the role of cluster master before all

standby nodes have rejoined the group. If this happens, you may stop waiting and proceed directly to step 4.

4. Upgrade the master node in the HA group according to steps 1-10 in "Upgrading Operating System Software".

Upgrading MLNX-OS Software on Modular Switches

Note

Modular switches feature dual management modules.

1. Identify the chassis HA master. Run:

```
show chassis ha
```

2. Upgrade the chassis master according to steps 1-8 in "Upgrading Operating System Software". Please DO NOT reboot!

3. Upgrade the second management module according to steps 1-8 in "Upgrading Operating System Software". Please DO NOT reboot!

4. Reset the slave management module. In the master management module, run:

```
chassis ha reset other
```

5. After invoking the command above, please reboot the master management immediately. Run:

```
reload force immediate
```

> **Note**
>
> An alternative for steps 4 and 5 is to power cycle the system.

6. Check that “reset count” equals 0 or 1. Run:

```
show chassis ha
```

If the reset count is not equal to either 0 or 1, power cycle the system.

7. Verify all the systems are back online as members of the IB subnet ID. Run:

```
show ib smnodes {brief}
```

> **Note**
>
> Using a modular switch with different software versions on its two management boards is not supported.
>
> When replacing a management board the software running on the replacement board must be aligned with the version of the software running on the other management board.

Deleting Unused Images

To delete unused images, conduct the following steps.

1. Get a list of the unused images.

```
switch (config) # show images

Installed images:
  Partition 1:
    version: image-X86_64-3.6.5000.img

  Partition 2:
    version: image-X86_64-3.6.5000.img

Last boot partition: 1
Next boot partition: 1

Images available to be installed:
  No image files are available to be installed.

Serve image files via HTTP/HTTPS: no

No image install currently in progress.
Boot manager password is set.

Image signing              : trusted signature always
required
Admin require signed images: yes

Settings for next boot only:
```

```
Fallback reboot on configuration failure: yes (default)
```

2. Delete the unused images.

```
switch (config) # image delete image-X86_64-3.9.1302.img
```

> **Note**
>
> When deleting an image, it is recommended to delete the file, but not the partition, so as to not overload system resources.

Downgrading OS Software

Prior to downgrading software, please make sure the following prerequisites are met.

1. Log in to the switch via the CLI using the console port.
2. Backup configuration by following these steps.
    1. Disable paging of CLI output.

        ```
        switch (config)# no cli default paging enable
        ```

    2. Display commands to recreate current running configuration.

        ```
        switch (config)# show running-config
        ```

    3. Copy the output to a text file.

Downloading Image

1. Log in to your system to obtain its product number.

    ```
    switch (config) # show inventory
    ```

2. Log in to NVIDIA Enterprise Support Portal and download the relevant MLNX-OS version to your system type
3. Log in to your system via the CLI.
4. Change to Config mode.

```
switch > enable
switch # configure terminal
switch (config) #
```

5. Delete all previous images from the Images available to be installed prior to fetching the new image.

6. Fetch the desired software image.

```
switch (config) # image fetch
scp://username:password@192.168.10.125/var/www/html/<image_name>
100.0%
[#############################################################
```

Downgrading Image

> **Note**
>
> The procedure described below assumes that booting and running is done from Partition 1 and the downgrade procedure is performed on Partition 2.

1. Log in to your system via the CLI as admin.

2. Enter config mode.

```
switch > enable
switch # configure terminal
```

3. Display all image files on the system.

```
switch (config) # show images
Images available to be installed:
new_image.img
 <downgrade version> 2010-09-19 16:52:50
Installed images:
Partition 1:
 <current version> 2010-09-19 03:46:25
Partition 2:
 <current version> 2010-09-19 03:46:25
Last boot partition: 1
Next boot partition: 1
No boot manager password is set.
```

4. Install the fetched image.

```
switch (config) # image install <image_name>
Step 1 of 4: Verify Image
100%
[##############################################################
Step 2 of 4: Uncompress Image
100.0%
[##############################################################
Step 3 of 4: Create Filesystems
100.0%
[##############################################################
Step 4 of 4: Extract Image
100.0%
[##############################################################
```

5. Display all image files on the system.

```
switch (config) # show images
Images available to be installed:
new_image.img
 <downgrade version> 2010-09-19 16:52:50
Installed images:
Partition 1:
 <current version> 2010-09-19 03:46:25
Partition 2:
 <downgrade version> 2010-09-19 16:52:50
Last boot partition: 1
Next boot partition: 2
No boot manager password is set.
```

6. Configure the boot location to be the other (next) partition.

```
switch (config) # image boot next
```

Note

There are two installed images on the system. Therefore, if one of the images gets corrupted (due to power interruption, for example), in the next reboot the image will go up from the second partition.

Note

If you are downgrading to an older software version which has never been run yet on the switch, use the following command sequence as well.

```
switch (config) # no boot next fallback-reboot
enable
switch (config) # configuration write
```

7. Reload.

```
switch (config) # reload
```

Switching to Partition with Older Software Version

The system saves a backup configuration file when upgrading from an older software version to a newer one. If the system returns to the older software partition, it uses this backup configuration file.

> ⚠ **Warning**
>
> All configuration changes done with the new software are lost when returning to the older software version.

There are 2 instances where the backup configuration file does not exist:

- The user has run “reset factory” command, which clears all configuration files in the system
- The user has run “configuration switch-to” to a configuration file with different name then the backup file

> ⓘ **Note**

Note that the configuration file becomes empty if the system is downgraded to a software version which has never been installed yet.

To allow switching partition to the older software version for the 2 aforementioned cases only, follow the steps below.

1. Run the following command.

```
switch (config)# no boot next fallback-reboot enable
```

2. Set the boot partition.

```
switch (config)# image boot next
```

3. Save the configuration.

```
switch (config)# configuration write
```

4. Reload the system.

```
switch (config)# reload
```

Upgrading System Firmware

MLNX-OS software package version has a default switch firmware version. When you update the operating system software to a new version, an automatic firmware update process will be attempted by MLNX-OS. This process is described below.

After Updating Software

Upon rebooting your switch system after updating the OS software, the OS compares its default firmware version with the currently programmed firmware versions on all the switch modules(leafs and spines on modular-class switches, or simply the switch card on modular switch systems).

If one or more of the switch modules is programmed with a firmware version other than the default version, then the OS automatically attempts to burn the default firmware version instead.

> **Note**
>
> If a firmware update takes place, then the login process is delayed a few minutes.

To verify that the firmware update was successful, log into your switch and run the command “show asic-version” (can be run in any mode). This command lists all of the switch modules along with their firmware versions. Make sure that all the firmware versions are the same and match the default firmware version. If the firmware update failed for one or more modules, then the following warning is displayed.

Some subsystems are not updated with a default firmware.

> **Note**
>
> If you detect a mismatch in firmware version for one or more modules of the switch system, please contact your assigned field application

engineer.

After Inserting a Switch Spine or Leaf

Note

This section is applicable to modular switch systems only.

If you insert a switch spine or leaf with a firmware version other than the default version of MLNX-OS, an automatic firmware update process takes place immediately to the inserted module *only*.

Note

The firmware update may take a few minutes. It is recommended not to run any commands until the firmware update completes.

Note

During firmware upgrade internal link status (up/down) notifications may be sent.

To verify that the firmware update was successful, run the command “show asic-version” (can be run in any mode). Check that the firmware version of the inserted switch spine or leaf has the default firmware version.

Note

If you detect a firmware version mismatch for the newly inserted module, please contact your assigned field application engineer.

Importing Firmware and Changing the Default Firmware

To perform an automatic firmware update by the OS for a different switch firmware version without changing the OS version, import the firmware package as described below. The OS sets it as the new default firmware and performs the firmware update automatically as described in the previous subsections.

Default Firmware Change on Standalone Systems

1. Import the firmware image (.mfa file).

```
switch (config) # image fetch scp://root@1.1.1.1:/tmp/fw-SIB-rel-11_1600_0200-FIT.mfa
Password (if required): *******
100.0%
[############################################################
switch (config) # image default-chip-fw fw-SIB-rel-11_1600_0200-FIT.mfa
Installing default firmware image. Please wait...
Default Firmware 11.1600.0200 updated. Please save
configuration and reboot for new FW to take effect.
```

2. Save the configuration.

```
switch (config) # configuration write
```

3. Reboot the system to enable auto update.

Default Firmware Change Dual Management Systems

This flow should be implemented on both management modules in parallel.

1. Import the firmware image (.mfa file) on both management modules. Run:

```
switch (config) # image fetch
scp://username:password@10.7.34.115//my_directory/fw-SIB-rel-11_1600_0200-FIT.mfa
  100.0%
[############################################################
```

2. Change default firmware on the management modules using the command image default-chip-fw.

3. Verify that both master and slave have successfully installed the new firmware. The following message should be displayed:

```
Default firmware <fw> updated. Please save configuration and
reboot for new FW to take effect.
```

4. Run "configuration write" on both management modules.

5. Run "chassis ha reset other" on the master management module only.

6. Run "reload" on the master management module.

Software Management Commands

image boot

	image boot {location <location-ID> | next} Specifies the default location where the system should be booted from.	
Syntax Description	location-ID	Specifies the default destination location. There can be up to 2 images on the system. The possible values are 1 or 2.
	next	Sets the boot location to be the next once after the one currently booted from, thus avoiding a cycle through all the available locations.
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # image boot location 2	
Related Commands	show images	
Notes		

boot next

	boot next fallback-reboot enable no boot next fallback-reboot enable Sets the default setting for next boot. Normally, if the system fails to apply the configuration on startup (after attempting upgrades or downgrades, as appropriate), it will reboot to the other partition as a fallback.

	The no form of the command tells the system not to do that, only for the next boot.
Syntax Description	N/A
Default	N/A
Configuration Mode	config
History	3.2.0506
Example	switch (config) # boot next fallback-reboot enable
Related Commands	show images
Notes	• Normally, if the system fails to apply the configuration on startup (after attempting upgrades or downgrades, as appropriate) it reboots to the other partition as a fallback. • The no form of this command tells the system not to do that only for the next boot. In other words, this setting is not persistent and goes back to being enabled automatically after each boot. • When downgrading to an older software version which has never been run yet on a system, the “fallback reboot” always happens, unless the command “no boot next fallback-reboot enable” is used. However, this also happens when the older software version has been run before, but the configuration file has been switched since upgrading. In general, a downgrade only works (without having the fallback reboot forcibly disabled) if the process can find a snapshot of the configuration file (by the same name as the currently active one) which was taken before upgrading from the older software version. If that is not found, a fallback reboot is performed in preference to falling back to the initial database because the latter generally involves a loss of network connectivity, and avoiding that is of paramount importance.

boot system

	boot system {location | next} no boot system next Configures which system image to boot by default.

	The no form of the command resets the next boot location to the current active one.	
Syntax Description	location	Specifies location from which to boot system • 1—installs to location 1 • 2—installs to location 2
	next	Boots system from next location after one currently booted
Default	N/A	
Configuration Mode	config	
History	3.2.0506	
Example	switch (config) # boot system location 2	
Related Commands	show images	
Notes		

image default-chip-fw

	image default-chip-fw <filename> no image default-chip-fw <original-fw-filename> Sets the default firmware package to be installed. The no form of the command resets default firmware package.	
Syntax Description	filename	Specifies the firmware filename
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
	3.6.6000	Added the no form of the command
Example	switch (config) # image default-chip-fw <filename>.mfa	
Related Commands	show asic-version show images	
Notes		

image delete

	image delete <image-name> Deletes the specified image file.	
Syntax Description	image-name	Specifies the image name
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # image delete <filename>.img	
Related Commands	show images	
Notes		

image fetch

	image fetch <URL> [<filename>] Downloads an image from the specified URL or via SCP.	
Syntax Description		
	URL	HTTP, HTTPS, FTP, TFTP, SCP and SFTP are supported Example: scp://username[:password]@hostname/path/filename
	filename	Specifies a filename for this image to be stored as locally
Default	N/A	
Configuration Mode	config	
History	3.1.0000 3.9.2000—Added VRF option	
Example		
switch (config) # image fetch scp://<username>@192.168.10.125/var/www/html/<image_name> Password ****** 100.0%[##] switch (config) #		

Other options: switch (config) # image fetch http://10.1.0.40/path/filename switch (config) # image fetch http://[fd4f:13:cc00:1::40]/path/filename switch (config) # image fetch ftp://user:mypassword@10.1.0.40/foo/bar.img switch (config) # image fetch ftp://user:mypassword@[fd4f:13:cc00:1::40]/foo/bar.img switch (config) # image fetch tftp://hostname/dir/filename switch (config) # image fetch tftp://[fd4f:13:cc00:1::40]/dir/filename switch (config) # image fetch scp://user@myhost/dir/filename switch (config) # image fetch scp://user@myhost:1022/dir/filename switch (config) # image fetch scp://user:pass@[fd4f:13:cc00:1::40]/dir/filename switch (config) # image fetch sftp://user@myhost/dir/filename switch (config) # image fetch sftp://user@[fd4f:13:cc00:1::40]:1022/dir/filename switch (config) # image fetch sftp://user:pass@[fd4f:13:cc00:1::40]/dir/filename	
Related Commands	show images
Notes	• Please delete the previously available image, prior to fetching the new image • The path to the file in the case of TFTP depends on the server configuration. Therefore, it may not be an absolute path but a relative one. • See "Upgrading Operating System Software" page

image install

	image install <image-filename> [location <location-ID>] | [progress <prog-options>] Installs the specified image file.	
Syntax Description	image-filename	Specifies the image name
	location-ID	Specifies the image destination location
	prog-options	• “no-track” overrides CLI default and does not track the installation progress • “track” overrides CLI default and tracks the installation progress
Default	N/A	
Configuration Mode	config	
History	3.1.0000	

Example	switch (config) # image install X86_64 3.6.5000 2017-07-26 06:54:12 x86_64 Step 1 of 4: Verify Image 100.0% [##] Step 2 of 4: Uncompress Image 100.0% [##] Step 3 of 4: Create Filesystems 100.0% [##] Step 4 of 4: Extract Image 100.0% [##] switch (config) #
Related Commands	show images
Notes	• The image cannot be installed on the “active” location (the one which is currently being booted) • On a two-location system, the location is chosen automatically if no location is specified

image move

	image move <src-image-name> <dest-image-name> Renames the specified image file.	
Syntax Description	src-image-name	Specifies the current image name
	dest-image-name	Specifies the new image name
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # image move image1.img image2.img	

Related Commands	show images
Notes	

image options

	image options serve all no image options serve all Configures options and defaults for image usage. The no form of the command disables options and defaults for image usage.	
Syntax Description	serve all	Specifies that the image files present on this appliance should be made available for HTTP and/or HTTPS download
Default	N/A	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # image options serve all	
Related Commands	show images	
Notes	The parameter “serve all” affects not only the files currently present, but also any files that are later downloaded. It only applies to image files, not the installed images, which are not themselves in a downloadable format. After running “serve all” the URLs where the images will be available are: • http://<HOSTNAME>/system_images/<FILENAME> • https://<HOSTNAME>/system_images/<FILENAME>	

show bootvar

	show bootvar Displays the installed system images and the boot parameters.
Syntax	N/A

Description	
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Example	switch (config)# show bootvar Installed images: Partition 1: X86_64 3.6.4110-12 2017-07-26 06:54:12 x86_64 Partition 2: X86_64 3.6.4006 2017-07-03 16:17:39 x86_64 Last boot partition: 1 Next boot partition: 1 Serve image files via HTTP/HTTPS: no Boot manager password is set. Image signing: trusted signature always required Admin require signed images: yes Settings for next boot only: Fallback reboot on configuration failure: yes (default)
Related Commands	
Notes	

show images

	show images Displays information about the system images and boot parameters.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Example	switch (config)# show images

	Installed images: Partition 1: X86_64 3.6.4110-12 2017-07-26 06:54:12 x86_64 Partition 2: X86_64 3.6.4006 2017-07-03 16:17:39 x86_64 Last boot partition: 1 Next boot partition: 1 Images available to be installed: webimage.tbz X86_64 3.6.4071-12 2017-07-26 06:54:12 x86_64 Serve image files via HTTP/HTTPS: no No image install currently in progress. Boot manager password is set. Image signing: trusted signature always required Admin require signed images: yes Settings for next boot only: Fallback reboot on configuration failure: yes (default)
Related Commands	show images
Notes	

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation (“NVIDIA”) makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer (“Terms of Sale”). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.