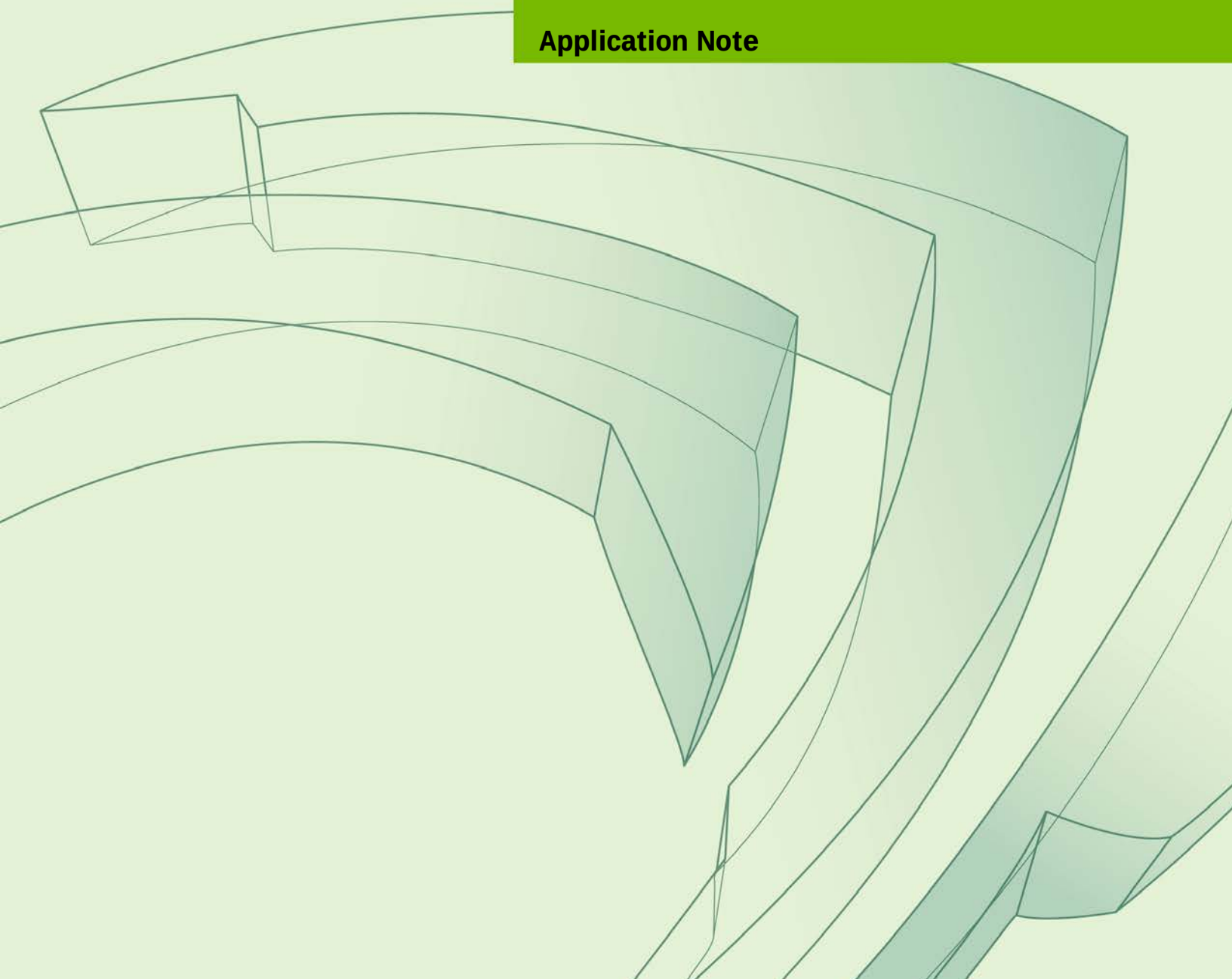
NVIDIA

NVIDIA JETSON TX1 FUSE SPECIFICATION

DA-08191-001_v06 | May 2018

Application Note



DOCUMENT CHANGE HISTORY

DA-08191-001_v06

Version	Date	Description of Change
01	August 30, 2016	Initial Release
02	October 26, 2016	Updated “Fuse Variables” section
03	May 5, 2017	•Updated Table 1 •Revised sections within the document
04	June 7, 2017	•Updated Table 1 •General update within the document
05	September 8, 2017	Updated “ARM Debug Authentication Signals” section
06	May 23, 2018	Updated note in Table 1

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

This application note provides a technical overview of the issues and considerations related to the NVIDIA® Jetson™ TX1 Fuse Specification.

NVIDIA Jetson TX1 includes customer/Original Device Manufacturer (ODM)-programmable fuses which are used to store security keys and ODM system design configuration options. Fuses are divided into 2 distinct areas:

- Manufacturing Fuses (For example; security keys, boot options, etc.)
- ODM Field Fuses (For example; defined by software for rollback protection, etc.)

Each logical fuse setting (except for spare fuses) is controlled by two physical fuses that are programmed simultaneously. This embedded hardware redundancy ensures that the programmed fuse state is read correctly after power-on reset. A similar redundancy is performed in software for spare fuses. All fuses default values are Logic 0 when not programmed. After they are programmed they represent a Logic 1.

SYSTEM REQUIREMENTS

Jetson TX1 contains all of the power and logic to program the onboard fuses. The system designer does not have to make any provision on their own system design.

FUSE VARIABLES

Jetson TX1 contains the following 2 types of fuses for ODM use.

- Those that configure the device and should be programmed during the manufacturing process before the product is released to the end user.
- Those that may be programmed during the lifetime of the product by the ODM for software to use. An example of this is to increment a value for software updates to prevent users from using a previous version of software or storing a serial number or date of first use.

MANUFACTURING PROGRAMMABLE FUSES

Jetson TX1 contains multiple manufacturing fuses that control different items for security and boot. These fuses should be programmed during the manufacturing process. The ODM Production Mode fuse (AKA Security Mode) should always be programmed by the ODM on the manufacturing line before the product is shipped to the end user. This fuse acts as a master lock for all of the manufacturing fuses. Once programmed, it locks the values of the other manufacturing fuses. They cannot be programmed once the ODM Production Mode fuse has been programmed.

Table 1 summarizes available fuse settings and values for each.

Note: All ODM fuses have the value of ZEROs when shipped to a customer.

CAUTION: Programming a fuse (changing the value of a fuse from 0 to 1) is non-reversible. Once a fuse bit is programmed (set to 1), you cannot change the fuse value from 1 to 0. For example: A value of 1 (0x0001) can be changed to 3 (0x0011) or 7 (0x0111). It cannot however be changed to a value of 4 (0x0100) since bit zero is already programmed to 1.

The burning of fuses should be done without a system reset between different phases.

Table 1. Fuse Name and Descriptions

Fuse Name	Fuse Description	Bit Length	Notes
FUSE_SECURITY_MODE [0]	**ODM Production Mode** Also known as ODM Security Mode. This fuse write-protects all manufacturing device fuses against any further fuse programming and also hides the SBK and DK values. **This fuse must be programmed last.**	1	
FUSE_ARM_JTAG_DIS [0]	**ARM JTAG Disable** Disables future use of ARM JTAG debug port. When this fuse is programmed, access to the ARM JTAG debug port is permanently disabled.	1	Note 3
FUSE_ODM_INFO[12:8]	**ARM Debug Authentication** Provides fine control of ARM debug capabilities Programming one of these fuses permanently disables the equivalent debug capability (refer to DFD documentation for details): •Bit 12 forces dbgen to 0 •Bit 11 forces niden to 0 •Bit 10 forces spiden to 0 •Bit 9 forces spniden to 0 •Bit 8 forces deviceen to 0	5	Note 3
FUSE_PRIVATE_KEY0 [31:0] /../ FUSE_PRIVATE_KEY3 [31:0]	**Secure Boot Key (SBK)** Stores an ODM-supplied secure boot key for each chip. Used in conjunction with the DK to create a Secure Storage Key (SSK). Example: “0xABCDEF” input value will be represented as “0x00000000000000000000000000ABCDEF”	128	Notes 1, 3, and 4

Fuse Name	Fuse Description	Bit Length	Notes
FUSE_PRIVATE_KEY4 [31:0]	**Device Key (DK)** Stores an ODM-supplied device key for each chip. Used in conjunction with the SBK to create a Secure Storage Key. Example: "0x1234" input value will be represented as "0x00001234"	32	Notes 3, and 4
FUSE_PUBLIC_KEY0 [31:0] /../ FUSE_PUBLIC_KEY7 [31:0]	**Public Key Hash (PKC)** Stores the hash of a public key provided by the ODM. Storing the hash allows to authenticate the full key.	256	Note 3
FUSE_RESERVED_SW [3]	**Skip Boot Device Selection Straps** Ignores the device selection straps and chooses the secondary boot device from the fuses when set.	1	Note 3
FUSE_RESERVED_SW [2:0]	**Boot Device Selection** Identifies the OS image boot device. Enumerated value read by the internal boot ROM.	3	Notes 2, and 3
FUSE_BOOT_DEVICE_INFO [13:0]	**Boot Device Configuration** Identifies the OS image boot device configuration. Used in conjunction with the Boot Device Selection to provide its configuration.	14	Notes 2, and 3
FUSED_RESERVED_SW [4]	**Enable Charger Detect** Used to enable charger detect.	1	Note 3
FUSE_RESERVED_SW [5]	**Watchdog Enable** Used to enable watchdog.	1	Note 3
FUSE_PKC_DISABLE [0]	**PKC Disable** Disable the use of Public Key Cryptography**.**	1	Note 3

Notes:

1. The SBK is not active to encrypt objects such as the boot loader, CFG, etc. until the ODM Production Mode fuse is programmed. Even if these entries are non-zero, the value is valid and can be read back (For example, used for SSK calculation). After ODM production fuse is programmed and a subsequent reset, the SBK value cannot be read back.
2. See the "Boot Options Fuse Configuration" table for the correct boot settings for your platform.
3. Fuse programming of ODM manufacturing programmable fuses is disabled when ODM Production Mode fuse = 1.
4. After programming the value and rebooting the chip, the value is an input to the SSK calculation regardless of whether the ODM Production Mode fuse has been set.

ODM Production Mode

The ODM production fuse is a global lock of all the manufacturing fuses. It should be programmed last in the manufacturing process after all other manufacturing fuses are programmed.

ARM JTAG Disable

When programmed, this fuse permanently prevents any JTAG access to the debug access port that occurs through the JTAG pins on Jetson TX1. This prevents any JTAG access by external ARM debuggers during normal product lifetime.

Note: Boundary Scan is still possible through the JTAG pins, irrespective of this fuse state.

ARM Debug Authentication Signals

These fuses control the standard ARM debug authentication signals; each fuse forces the corresponding signal to 0 (disabled). Table 2 describes the ARM debug authentication signals.

Table 2. ARM Debug Authentication Signals

Signal Name	Description	Definition	Common Usecase
DBGEN	**Debug Enable** When asserted, enables invasive and non-invasive debug of non-secure state. Note that when DBGEN is not asserted, access to debug components is generally still permitted, but those components are disabled.	NonSecure Invasive Debug Enable	CPUs to halt AXIAP to make system accesses ETR to stream trace to DRAM
NIDEN	**Non-Invasive Debug Enable** When asserted, enables non-invasive debug operations, such as trace, of non-secure state. NIDEN can be asserted independently of DBGEN.	NonSecure Non Invasive Debut Enable	PTM trace from CPUs
SPIDEN	**Secure Privileged Invasive Debug Enable** When asserted along with DBGEN, enables invasive and non-invasive debug of Secure state.	Secure Invasive Debug Enable	AXI_AP to make secure accesses into the system ETR to write to Secure DRAM

Signal Name	Description	Definition	Common Usecase
SPNIDEN	**Secure Privileged Non-Invasive Debug Enable** When asserted along with NIDEN, enables non-invasive debug of Secure state.	Secure NonInvasive Debug Enable	Accessing Secure registers in PMU and CPUs over the Debug APB
DEVICEEN	**Device Debug Enabled** Enables connection of external debug tools to the device. This signal also drives the DBGSWENABLE, which is an enable input signal of the CoreSight Components and Cortex-A Series processor.	Device Enable	Accessing any registers on mapped over the Debug APB

Secure Boot Key

These fuses should be programmed with the secure boot key if SBK is being used. The SBK only takes effect once the ODM production mode fuse has been programmed.

Device Key

These fuses should be programmed with the ODMs device key and used to create a secure storage key (SSK). The device key (DK) only takes effect once the ODM production mode fuse has been programmed.

Public Key Hash

These fuses should be programmed with the hash of the ODM public key. It only takes effect once the ODM production mode fuse has been programmed.

Skip Boot Device Selection Straps

This fuse determines if the boot device selection is determined by the straps or by the boot device fuse settings.

Jetson TX1 is supplied as configured to boot from straps. For production devices, it is recommended that the fuses are used to select the boot device. When this fuse is programmed then the boot device is determined by the setting of the Boot Device Selection fuses.

Boot Device Selection

Jetson TX1 uses eMMC for boot. These fuses should remain at their default (0x0 = eMMC).

Table 3. Boot Device Selection (FUSE_RESERVED_SW[2:0])

Register	Description	Values
FUSE_RESERVED_SW [2:0]	Boot Device Select	0x0 = eMMC
		0x1 – 0x7 Reserved

Boot Device Information

These fuses determine parameters for the boot device. Jetson TX1 uses eMMC for boot. These fuses should be programmed to 0x0011 (eMMC x8, No DDR, Query Voltage, Boot Mode off, 25.5 MHz, 1.8V, 512 Byte Page size) if boot fuses are to be programmed.

Table 4. Boot Device Configuration (FUSE_BOOT_DEVICE_INFO [13:0])

Device	Fuse Bits	Description	Values
eMMC	13	Reserved	Ignored; set to 0x0
	12:10	MultiPage support	0x0 = default Single page read (512 Byte)
			0x1 = Multi 2 page read (1024 Byte)
			0x2 = Multi 4 page read (2048 Byte)
			0x3 = Multi 8 page read (4096 Byte)
			0x4 = Multi 16 page read (8192 Byte)
			0x5 - 0x7 = reserved
	9:6	Clock Divider PLLP clock at 408 MHz* * See Boot section of TRM ** Can be SDR or DDR; Select via DDR Mode Selection bit.	0x0 = default clock divider 16 (clock at 25.5 MHz)
			0x1 = clock divider 8 (clock at 51MHz) **
			0x2 = clock divider 2.5 (clock at 163.2 MHz)
			Reserved
			Reserved
			Reserved
			Reserved
			Reserved
			Reserved
			Reserved
	5	VDDIO_SDMMC4 Pads voltage	0x0 = 1.8v (power on default)
			0x1 = 1.2v
	4	Disable Boot Mode	0x0 = Boot mode On
			0x1 = Boot mode Off

Device	Fuse Bits	Description	Values
	3:2	Voltage Range	0x0 = Query Voltage
			0x1 = High Voltage
			0x2 = Dual Voltage
			0x3 = Low Voltage
	1	DDR Mode Selection	0x0 = Normal
			0x1 = DDR
	0	Data bus width	0x0 = 4 bits
			0x1 = 8 bits

Watchdog Enable

This fuse when programmed enables the internal watchdog during boot. Refer to the TRM for more information.

PKC Disable

This fuse selects between using PKC or the SBK for secure booting method. However, SBK boot is obsolete and not used anymore.

Table 5. PKC Disable (FUSE_PKC_DISABLE [0])

FUSE_PKC_DISABLE = 0b (Default)	FUSE_PKC_DISABLE = 1b
The PKC secure boot is selected. Read the 2048-bit public key from boot media and authenticate it against the corresponding 256-bit SHA hash of the public key in fuses; the public key is used to authenticate all subsequent boot components.	The SBK (AES) secure boot is selected. Read the 128-bit SBK from fuses; the SBK is used to authenticate all subsequent boot components.

ODM FIELD PROGRAMMABLE FUSES

The following fuses are available for the system designer to use for programming during the product lifetime. If these fuses are to be altered, then the fuse programming voltage VPP_FUSE must be present in the system at the time the fuses are to be programmed.

The RESERVED_ODM fuses are split into 8 banks of 32 bits. The first of these 4 banks (0-3) can be locked out by setting the corresponding bit in the ODM Lock fuse (For example, to lock RESERVED_ODM bank 1, then ODM_LOCK bit [1] should be set). This will prevent any unintentional programming of other bits in this bank.

RESERVED_ODM banks 4-7 do not have this protection feature.

Table 6. Field Programmable Fuses

Fuse Name	Fuse Description	Bit Length
Reserved ODM (FUSE_RESERVED_ODM0 [31:0]) /../ (FUSE_RESERVED_ODM7 [31:0])	Customer programmable fuses. One anticipated application of the Reserved ODM fuses is software version revocation, although their use is solely at the discretion of the customer. The Reserved ODM fuses remain programmable after the ODM Production Mode fuse has been programmed.	256
ODM_lock (FUSE_ODM_LOCK [3:0])	When FUSE_ODM_LOCK[n] is programmed it disables further changes to the FUSE_RESERVED_ODMn[31:0] fuses. Only the first 4 blocks of ODM fuses can be locked FUSE_ODM_LOCK [0] Locks FUSE_RESERVE_ODM0[31:0] FUSE_ODM_LOCK [1] Locks FUSE_RESERVE_ODM1[31:0] FUSE_ODM_LOCK [2] Locks FUSE_RESERVE_ODM2[31:0] FUSE_ODM_LOCK [3] Locks FUSE_RESERVE_ODM3[31:0]	4

Note: Refer to *Jetson Device Secure Boot and Fuse Burning README and Tools* for information on how to program the fuses.

Notice

The information provided in this specification is believed to be accurate and reliable as of the date provided. However, NVIDIA Corporation (“NVIDIA”) does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information. 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 publication supersedes and replaces all other specifications for the product that may have been previously supplied.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and other changes to this specification, at any time and/or to discontinue any product or service without notice. Customer should obtain the latest relevant specification 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. NVIDIA hereby expressly objects to applying any customer general terms and conditions with regard to the purchase of the NVIDIA product referenced in this specification.

Unless specifically agreed in writing by NVIDIA, 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 these specifications will be suitable for any specified use without further testing or modification. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to ensure the product is suitable and fit for the application planned by customer and to do 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 specification. NVIDIA does not accept any 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 specification, 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 specification. 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 specification is permissible only if reproduction is approved by NVIDIA in writing, is reproduced without alteration, and is accompanied by all associated conditions, limitations, and notices.

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. 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 NVIDIA terms and conditions of sale for the product.

ARM

ARM, AMBA and ARM Powered are registered trademarks of ARM Limited. Cortex, MPCore and Mali are trademarks of ARM Limited. All other brands or product names are the property of their respective holders. "ARM" is used to represent ARM Holdings plc; its operating company ARM Limited; and the regional subsidiaries ARM Inc.; ARM KK; ARM Korea Limited.; ARM Taiwan Limited; ARM France SAS; ARM Consulting (Shanghai) Co. Ltd.; ARM Germany GmbH; ARM Embedded Technologies Pvt. Ltd.; ARM Norway, AS and ARM Sweden AB.

Trademarks

NVIDIA, the NVIDIA logo, and Jetson 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.

Copyright