

» User Guide «

CP6004-SA
CP6004-RA
CP6004-RC
CP6004X-SA

uEFI BIOS

Doc. ID: 1053-6161, Rev. 3.0
August 13, 2013



Revision History

Publication Title:		CP6004-SA/-RA/-RC/CP6004X-SA uEFI BIOS User Guide
Doc. ID:		1053-6161
Rev.	Brief Description of Changes	Date of Issue
1.0	Initial issue based on the uEFI BIOS version R13	21-Dec-2012
2.0	General update based on uEFI BIOS version R14, added description for the CP6004X-SA	1-Feb-2013
3.0	Added description for the CP6004-RA/CP6004-RC based on uEFI BIOS version R14	13-Aug-2013

Imprint

Kontron Europe GmbH may be contacted via the following:

MAILING ADDRESS

Kontron Europe GmbH
Sudetenstraße 7
D - 87600 Kaufbeuren Germany

TELEPHONE AND E-MAIL

+49 (0) 800-SALESKONTRON
sales@kontron.com

For further information about other Kontron products, please visit our Internet web site: www.kontron.com.

Disclaimer

Copyright © 2013 Kontron AG. All rights reserved. All data is for information purposes only and not guaranteed for legal purposes. Information has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo and all other trademarks or registered trademarks are the property of their respective owners and are recognized. Specifications are subject to change without notice.



Table of Contents

<i>Revision History</i>	<i>ii</i>
<i>Imprint</i>	<i>ii</i>
<i>Disclaimer</i>	<i>ii</i>
<i>Table of Contents</i>	<i>iii</i>
1. Starting uEFI BIOS Setup	3
1.1 Main Setup Menu	4
1.2 Navigation	5
2. Main Setup	9
2.1 BIOS Information	9
2.2 Trusted Computing	10
2.2.1 TPM Configuration	10
2.2.1.1 TPM Support	10
2.2.1.2 TPM State	11
2.2.2 Pending TPM Operation	11
2.2.3 Current TPM Status Information	11
2.3 CPU Configuration	12
2.3.1 CPU Configuration	12
2.3.2 Max Freq Ratio	12
2.4 Firmware Update Configuration	13
2.4.1 Me FW Image Re-Flash	13
2.5 USB Configuration	14
2.5.1 USB Configuration	14
2.5.1.1 USB Devices	14
2.5.1.2 Legacy USB Support	14
2.5.1.3 EHCI Hand-Off	15
2.5.2 USB Hardware Delays and Time-outs	15
2.5.2.1 USB Transfer Timeout	15
2.5.2.2 Device Reset Timeout	15
2.5.2.3 Device Power-up Delay	15
2.6 Serial Port Console Redirection	16




- 2.6.1 COM0 16
 - 2.6.1.1 Console Redirection 16
 - 2.6.1.2 Console Redirection Settings 16
- 2.6.2 COM1 17
 - 2.6.2.1 Console Redirection 17
 - 2.6.2.2 Console Redirection Settings 17
- 2.6.3 Serial Port for Out-of-Band Management/Windows EMS 20
 - 2.6.3.1 Console Redirection 20
 - 2.6.3.2 Console Redirection Settings 21
- 2.7 Intel ICC 23
 - 2.7.1 Maximum supported frequency/Minimum supported frequency/etc. 23
 - 2.7.2 New SSC Mode 23
 - 2.7.3 New SSC spread percentage 23
 - 2.7.4 Apply settings immediately 24
 - 2.7.5 Apply settings permanently after reboot 24
- 2.8 System Language 24
- 2.9 System Date 24
- 2.10 System Time 24
- 2.11 Access Level 24

3. Boot Setup 27

- 3.1 Boot Configuration 27
 - 3.1.1 Setup Prompt Timeout 27
 - 3.1.2 Bootup NumLock State 28
 - 3.1.3 Quiet Boot 28
 - 3.1.4 Fast Boot 28
 - 3.1.5 CSM16 Module Version 28
 - 3.1.6 GateA20 Active 28
 - 3.1.7 Option ROM Messages 29
 - 3.1.8 Interrupt 19 Capture 29
- 3.2 Boot Option Priorities 29
 - 3.2.1 Boot Option #1..4 29
 - 3.2.2 Hard Drive/Network Device/CD/DVD ROM Drive/Floppy Drive/etc.... 29





4. Security Setup	33
4.1 Administrator Password	34
4.2 User Password	34
4.3 HDD Security Configuration	34
4.4 Remember the Password	34
5. Save & Exit	37
5.1 Save Changes and Exit	37
5.2 Discard Changes and Exit	37
5.3 Save Changes and Reset	37
5.4 Discard Changes and Reset	38
5.5 Save Changes (Save Options)	38
5.6 Discard Changes (Save Options)	38
5.7 Restore Defaults (Save Options)	38
5.8 Save as User Defaults (Save Options)	38
5.9 Restore User Defaults (Save Options)	38
5.10 Boot Override	38
6. The uEFI Shell	41
6.1 Introduction, Basic Operation	41
6.1.1 Shell Startup	41
6.2 Kontron Shell Commands	42
6.2.1 kBiosRevision uEFI Shell Command	43
6.2.2 kboardconfig uEFI Shell Command	44
6.2.3 kboardinfo uEFI Shell Command	51
6.2.4 kboot uEFI Shell Command	56
6.2.5 kbootnsh uEFI Shell Command	57
6.2.6 kclearnvram uEFI Shell Command	57
6.2.7 kflash uEFI Shell Command	58
6.2.8 kipmi uEFI Shell Command	59
6.2.9 kmkramdisk uEFI Shell Command	62
6.2.10 kpassword uEFI Shell Command	63
6.2.11 kresetconfig uEFI Shell Command	64



6.2.12	<i>kwdt uEFI Shell Command</i>	65
6.3	<i>uEFI Shell Scripting</i>	66
6.3.1	<i>Startup Scripting</i>	66
6.3.2	<i>Create a Startup Script</i>	66
6.3.3	<i>Examples of Startup Scripts</i>	66
6.3.3.1	<i>Automatic Booting from USB Flash Drive</i>	66
6.3.3.2	<i>Switch On Clock Spreading Prior to Booting from Harddrive</i>	66
6.3.3.3	<i>Execute Shell Script on Other Harddrive</i>	66
6.3.3.4	<i>Enable Watchdog and Control PXE Boot</i>	67
6.3.3.5	<i>Handling the Startup Script in the Flash Bank</i>	68
7.	<i>Updating the uEFI BIOS</i>	71
7.1	<i>uEFI BIOS Fail-Over Mechanism</i>	71
7.2	<i>Updating Procedure</i>	71
7.3	<i>uEFI BIOS Recovery</i>	71
7.4	<i>Determining the Active Flash</i>	71



Chapter

1

Starting uEFI BIOS Setup



This page has been intentionally left blank.





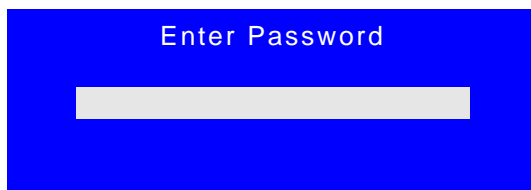
1. Starting uEFI BIOS Setup

The CP6004-SA/-RA/-RC/CP6004X-SA is provided with a Kontron-customized, pre-installed and configured version of Aptio® (referred to as uEFI BIOS in this manual), AMI's next generation BIOS firmware based on the Unified Extensible Firmware Interface (uEFI) specification and the Intel® Platform Innovation Framework for EFI.

This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the CP6004-SA/-RA/-RC/CP6004X-SA. To take advantage of these functions, the uEFI BIOS comes with an uEFI Shell, which provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration, and a Setup program, which allows the accessing of various menus that provide functions or access to sub-menus with more specific functions of their own. The individual menus and the configurable functions are described in this guide.

To start the uEFI BIOS Setup program, follow the steps below:

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the or the <F2> key.
4. If the uEFI BIOS is password-protected, a window such as the one below will appear:



Enter either the User password or the Administrator password (refer to Chapter 4, Security Setup, for further information), press <RETURN>, and proceed with step 2.

5. A Setup menu with the following token attributes will appear.
The currently active menu and the currently active uEFI BIOS Setup item are highlighted in white.



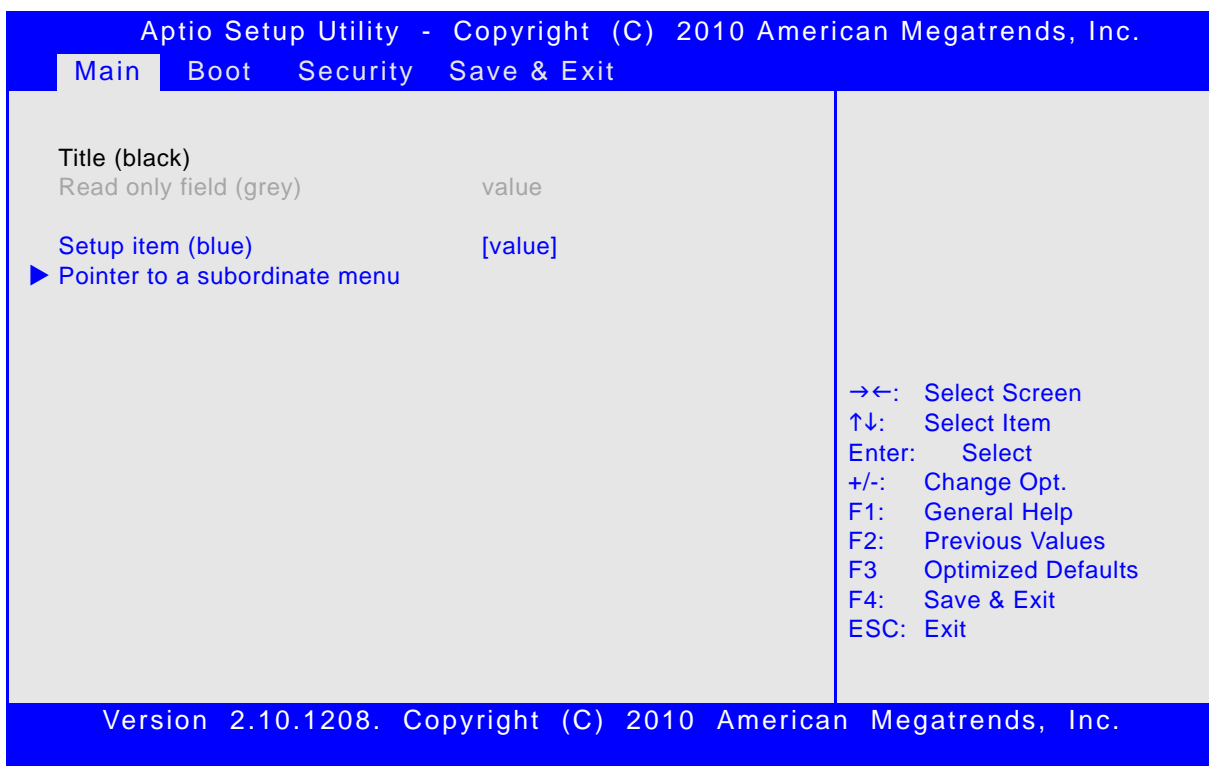
1.1 Main Setup Menu

The Main setup menu is the first screen that appears after starting the Setup program.

At the top of this screen and all of the other major screens, there is a setup menu selection bar, which permits access to all of the other major setup menus. These menus are selected via the left-right arrow keys.

All setup menu screens have two main frames. The left frame displays all the functions that can be configured. They are displayed in blue. Functions displayed in gray provide information about the status or the operational configuration.

The right frame displays the key legend. Above the key legend there is an area reserved for a text message. When a function is selected in the left frame, it is displayed in white. Often a text message will accompany it.





1.2 Navigation

The uEFI BIOS setup program uses a hot key-based navigation system. A hot key legend is located in the right frame on most setup screens. The following table provides information concerning the usage of these hot keys.

HOT KEY	DESCRIPTION
<F1>	The <F1> key is used to invoke the General Help window.
<F2>	The <F2> key is used to restore the previous values.
<F3>	The <F3> key is used to load the defaults.
<F4>	The <F4> key is used to save the current settings and exit the uEFI BIOS Setup.
→ ← Right/Left	The <i>Right and Left</i> <Arrow> keys are used to select a major Setup screen. For example: Main Screen, Advanced Screen, Chipset Screen, etc.
↑ ↓ Up/Down	The <i>Up and Down</i> <Arrow> keys are used to select a Setup function or a sub-screen.
+ - Plus/Minus	The <i>Plus and Minus</i> <Arrow> keys are used to change the field value of a particular Setup function, for example, system date and time.
<ESC>	The <ESC> key is used to exit a menu or the uEFI BIOS Setup. Pressing the <ESC> key in a sub-menu causes the next higher menu level to be displayed. When the <ESC> key is pressed in a major Setup menu, the uEFI BIOS Setup is terminated without saving any changes made.
<Enter>	The <Enter> key is used to execute a command or select a menu.



This page has been intentionally left blank.



Chapter **2**

Main Setup



This page has been intentionally left blank.



2. Main Setup

Upon entering the uEFI BIOS Setup program, the Main setup screen is displayed. This screen lists the main setup sub-screens and provides very basic system information as well as functions for setting the system time and date. In addition, the remaining major setup menus can be accessed from this screen. This screen can also be selected from any other major setup screen by using the Main tab.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main Boot Security Save & Exit

BIOS Information
 BIOS Vendor American Megatrends
 Core Version 4.6.5.1
 Compliance UEFI 2.3; PI 1.2
 Project Version B3D01 14.00 x64
 Build Date and Time 01/09/2013 09:50:41

Memory Information
 Memory Frequency 1600 Mhz
 Total Memory 8192 MB (DDR3)

▶ Trusted Computing
 ▶ CPU Configuration
 ▶ Firmware Update Configuration
 ▶ USB Configuration
 ▶ Serial Port Console Redirection
 ▶ Intel ICC

System Language [English]
 System Date [Fri 07/12/2012]
 System Time [13:47:26]
 Access Level Administrator

→←: Select Screen
 ↑↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F2: Previous Values
 F3: Optimized Defaults
 F4: Save & Exit
 ESC: Exit

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

2.1 BIOS Information

This function provides display-only information concerning the uEFI BIOS.

Information about the running uEFI BIOS version is reflected in the display-only function Project Version (parameter "14.00" indicates revision 14).



2.2 Trusted Computing

This screen provides functions for specifying the TPM configuration settings and TPM displaying status information.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Main

<p>TPM Configuration</p> <p>TPM Support [Enable]</p> <p>TPM State [Enabled]</p> <p>Pending TPM Operation [None]</p> <p>Current TPM Status Information</p> <p>TPM Enabled Status: [Enabled]</p> <p>TPM Active Status: [Activated]</p> <p>TPM Owner Status: [Owned]</p>	<p>→←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Exit</p> <p>ESC: Exit</p>
---	---

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

2.2.1 TPM Configuration

2.2.1.1 TPM Support

This function is used to provide the Trusted Platform Module (TPM) functionality to the OS.

Note: Trusted Platform Module support is available on request.

SETTING	DESCRIPTION
Disable	Use this setting to disable TPM support. If this setting is used, TPM is not present for the OS, regardless whether the function TPM State is enabled or not.
Enable	Use this setting to enable TPM support.

Default setting: Disable





2.2.1.2 TPM State

This function is used to select the TPM State command to be issued to the TPM after POST.

Note: This function is available only when the function TPM Support is set to Enable.

SETTING	DESCRIPTION
Disabled	Use this setting to disable the TPM after POST. If this setting is used, the TPM is present for the OS but its functionality is locked.
Enabled	Use this setting to enable the TPM after POST.

Default setting: Disabled

2.2.2 Pending TPM Operation

This function is used to select a TPM command to be issued once against the TPM during the next boot.

Note: This function is available only when the function TPM Support is set to Enable.

SETTING	DESCRIPTION
None	Use this setting to prevent the system from issuing any TPM commands.
Enable Take Ownership	Use this setting to allow the system to issue an Enable Take Ownership command during the next boot. If this setting is used, the Take Ownership command is enabled, which allows the OS to take ownership of the TPM.
Disable Take Ownership	Use this setting to allow the system to issue a Disable Take Ownership command during the next boot. If this setting is used, the Take Ownership command is disabled, which prevents the OS from taking ownership of the TPM.
TPM Clear	Use this setting to allow the system to issue a TPM Clear command during the next boot. If this setting is used, the TPM is reset to the factory default. Warning: Use of this setting also deletes any keys and passwords stored within the TPM. Always ensure that encryption software such as Microsoft BitLocker, etc. are deactivated prior to selecting this setting.

Default setting: None

2.2.3 Current TPM Status Information

This is a display-only function providing status information about the TPM.

FUNCTION	DESCRIPTION
TPM Enabled Status	Displays if the TPM device is enabled.
TPM Active	Displays if the TPM has been activated by the OS.
TPM Owner Status	Displays if the OS has taken ownership of the TPM device.



2.3 CPU Configuration

This screen provides information concerning the CPU operating frequencies and the ability to set the frequency ratio.

Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.

Main

CPU Configuration		
Inter (R) Core(TM) i7-3612QE CPU @ 2.10GHz		
Max CPU Speed	2100 MHz	
Min CPU Speed	1200 MHz	
CPU Speed	2100 MHz	
Max Freq Ratio	255	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.

2.3.1 CPU Configuration

This is a display-only function indicating general information about the installed CPU.

2.3.2 Max Freq Ratio

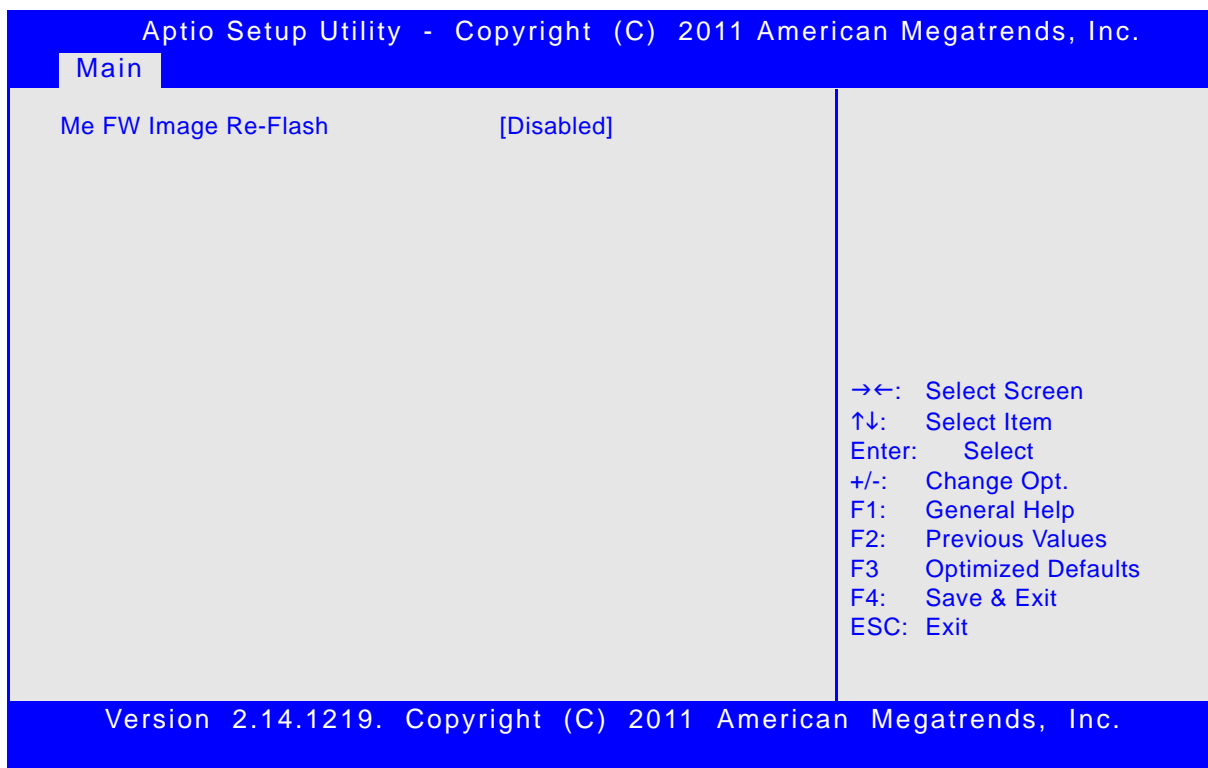
This function is used to permit the CPU frequency to be adjusted so as to make a reduction in power consumption possible when higher performance is not required.

To ensure that the maximum desired frequency is not exceeded, the CPU turbo mode must be disabled using the uEFI shell command "kboardconfig CpuTurbo disabled".



2.4 Firmware Update Configuration

This screen provides functions for specifying the firmware update configuration settings.



2.4.1 Me FW Image Re-Flash

This function is used to enable or disable Intel® Management Engine (ME) firmware re-flashing.

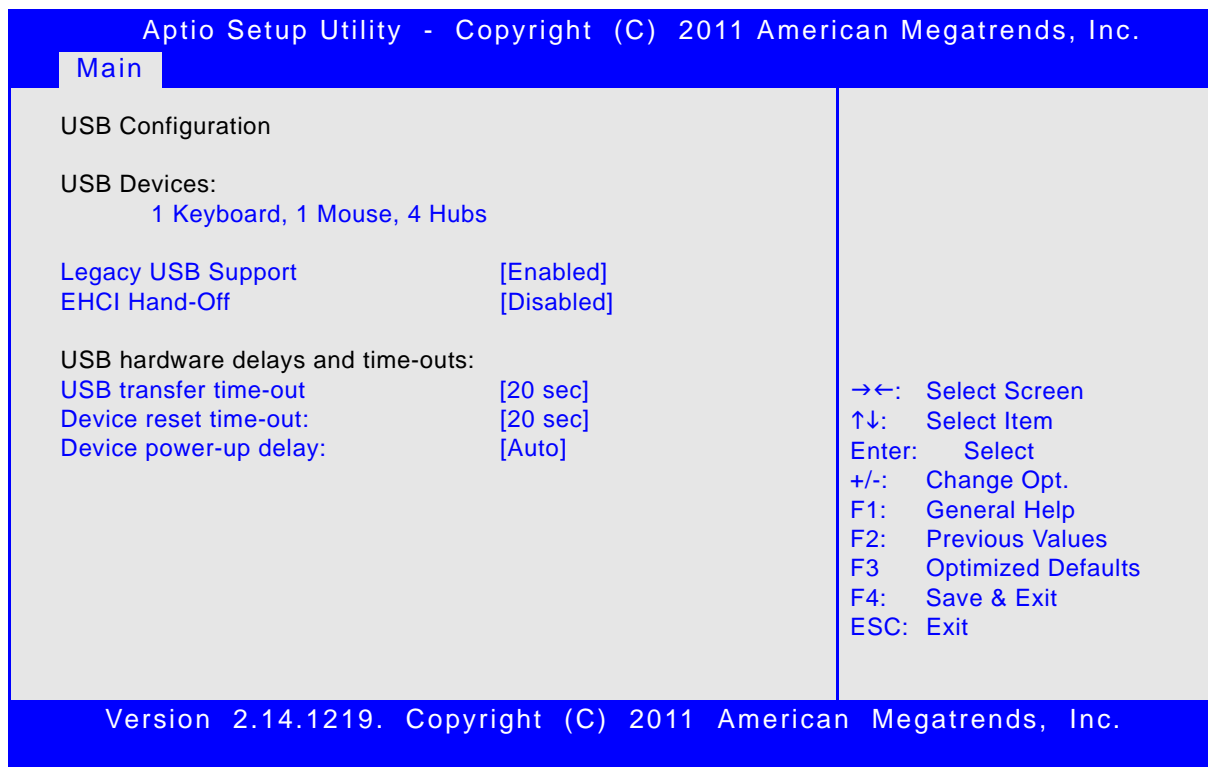
Note: Setting this function to Enabled sends a message to the ME firmware to be temporarily disabled for the next boot. However, after the next boot, this function shows Disabled.

SETTING	DESCRIPTION
Disabled	Use this setting to disable ME firmware re-flashing.
Enabled	Use this setting to enable ME firmware re-flashing when the whole uEFI BIOS image including a new ME-Firmware section must to be flashed.

Default setting: Disabled

2.5 USB Configuration

This screen provides information about support for USB devices as well as functions for specifying the USB configuration settings.



Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.

Main

USB Configuration

USB Devices:
1 Keyboard, 1 Mouse, 4 Hubs

Legacy USB Support [Enabled]
EHCI Hand-Off [Disabled]

USB hardware delays and time-outs:
USB transfer time-out [20 sec]
Device reset time-out: [20 sec]
Device power-up delay: [Auto]

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.

2.5.1 USB Configuration

2.5.1.1 USB Devices

This is a display-only function providing general information about the USB devices detected.

2.5.1.2 Legacy USB Support

This function is required for booting from USB devices and for operating systems which do not support USB themselves (mainly DOS and some BootLoaders).

SETTING	DESCRIPTION
Disabled	Use this setting to disable legacy USB support.
Enabled	Use this setting to enable legacy USB support.
Auto	Use this setting to enable legacy USB support if there are USB devices present.

Default setting: Enabled



2.5.1.3 EHCI Hand-Off

This function is used to enable a workaround for operating systems without EHCI Hand-Off support. The EHCI ownership change should be claimed by the EHCI driver.

SETTING	DESCRIPTION
Disabled	Use this setting to disable EHCI Hand-Off support.
Enabled	Use this setting to enable EHCI Hand-Off support.

Default setting: Disabled

2.5.2 USB Hardware Delays and Time-outs

2.5.2.1 USB Transfer Timeout

This function selects the timeout in seconds that the USB core will wait for Control, Bulk, and Interrupt transfers.

SETTING	DESCRIPTION
1 sec 5 sec 10 sec 20 sec	Use one of these settings to specify how long the USB core is to wait for Control, Bulk, and Interrupt transfers.

Default setting: 20 sec

2.5.2.2 Device Reset Timeout

This function selects the timeout in seconds that the POST will wait for a USB mass storage device to become ready after start unit command.

SETTING	DESCRIPTION
10 sec 20 sec 30 sec 40 sec	Use one of these settings to specify how long the POST will wait for a USB mass storage device to become ready after the start unit command.

Default setting: 20 sec

2.5.2.3 Device Power-up Delay

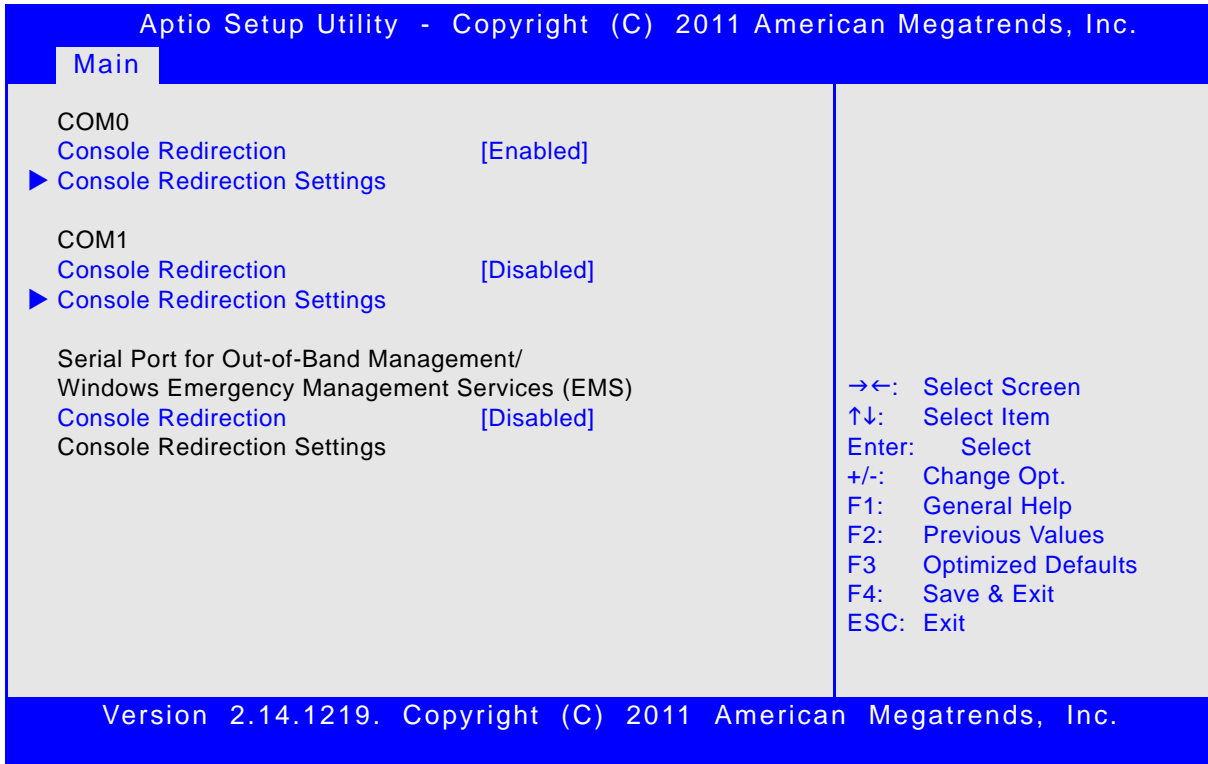
This function determines the maximum time the device will take before it properly reports itself to the Host Controller. "Auto" uses a default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor. If the "Manual" option is chosen, the device power up delay in seconds field will be enabled to accept a delay ranging from 1 to 40 seconds.

SETTING	DESCRIPTION
Auto	Use this setting to specify a default delay time for a Root or Hub port. (root port = 100ms; hub port = value in hub descriptor)
Manual	Use this setting to specify a delay time from 1 to 40 seconds. (contents of seconds field)

Default setting: Auto

2.6 Serial Port Console Redirection

This screen provides information about functions for specifying the Serial Port Console Redirection configuration settings. Console redirection can be used to remotely operate system settings and the uEFI console.



2.6.1 COM0

On the CP6004-SA/-RA/CP6004X-SA, the COM0 port (serial port 0) corresponds to the RS-232 serial port on the front panel (hardware designation COMA) and is switchable to rear I/O.

On the CP6004-RC, the COM0 port (serial port 0) corresponds to the RS-232 serial port on the rear I/O (hardware designation COMA).

2.6.1.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to disable console redirection for COMA (RS-232).
Enabled	Use this setting to enable console redirection for COMA (RS-232).

Default setting: Enabled

2.6.1.2 Console Redirection Settings

For information about this function, refer to Chapter 2.6.2.2 in this manual.



2.6.2 COM1

On the CP6004-SA/-RA/-RC/CP6004X-SA, the COM1 port (serial port 1) corresponds to the RS-422 serial port on the CompactPCI Rear I/O connector J3 (hardware designation COMB).

2.6.2.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to disable console redirection for COMB (RS-232).
Enabled	Use this setting to enable console redirection for COMB (RS-232).

Default setting: Disabled

2.6.2.2 Console Redirection Settings

This screen provides information about functions for specifying the Console Redirection configuration settings for the serial port 0 (COM0) and serial port 1 (COM1). Each serial port can be independently configured.

Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.

Main

COM0		
Console Redirection Settings		
Terminal Type	[ANSI]	
Bits per second	[115200]	
Data Bits	[8]	
Parity	[None]	
Stop Bits	[1]	
Flow Control	[None]	
VT-UTF8 Combo Key Support	[Enabled]	→←: Select Screen
Recorder Mode	[Disabled]	↑↓: Select Item
Resolution 100x31	[Disabled]	Enter: Select
Legacy OS Redirection Resolution	[80x24]	+/-: Change Opt.
Putty KeyPad	[VT100]	F1: General Help
Redirection After BIOS POST	[Always Enable]	F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit

Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.



2.6.2.2.1 Terminal Type

SETTING	DESCRIPTION
VT100	Use one of these settings to select the terminal type to be emulated.
VT100+	
VT-UTF8	
ANSI	

Default setting: ANSI

2.6.2.2.2 Bits per second

SETTING	DESCRIPTION
9600	Use one of these settings to select the baud rate of the serial port.
19200	
38400	
57600	
115200	

Default setting: 115200

2.6.2.2.3 Data Bits

SETTING	DESCRIPTION
7	Use one of these settings to specify the number of data bits per frame.
8	

Default setting: 8

2.6.2.2.4 Parity

SETTING	DESCRIPTION
None	Use one of these settings to select the parity for the serial port.
Even	
Odd	
Mark	
Space	

Default setting: None

2.6.2.2.5 Stop Bits

SETTING	DESCRIPTION
1	Use one of these settings to specify the number of stop bits for the serial port.
2	

Default setting: 1

2.6.2.2.6 Flow Control

SETTING	DESCRIPTION
None	Use one of these settings to specify the type of flow control to be used for this serial port.
Hardware RTS/CTS	

Default setting: None

2.6.2.2.7 VT-UTF8 Combo Key Support

Use this function to enable or disable VT-UTF8 Combination Key Support for ANSI/ VT100 terminals.

SETTING	DESCRIPTION
Disabled	Use this setting the disable combination key support.
Enabled	Use this setting the enable combination key support.

Default setting: Enabled

2.6.2.2.8 Recorder Mode

Use this function to specify whether display formatting characters are to be transmitted along with data or if only data is to be transmitted.

SETTING	DESCRIPTION
Disabled	Use this setting to specify normal terminal operation.
Enabled	Use this setting to specify that only text will be sent. Use this to capture terminal data.

Default setting: Disabled

2.6.2.2.9 Resolution 100x31

SETTING	DESCRIPTION
Disabled	Use this setting the disable extended terminal resolution.
Enabled	Use this setting the enable extended terminal resolution.

Default setting: Disabled

2.6.2.2.10 Legacy OS Redirection

SETTING	DESCRIPTION
80x24	Use one of these settings to select the number of rows and columns for legacy OS redirection.
80x25	

Default setting: 80x24



2.6.2.2.11 Putty KeyPad

SETTING	DESCRIPTION
VT100	Use one of the available settings to select the Function Key and the KeyPad when using Putty as terminal program. Ensure that the setting of this function is the same as the setting in the Putty terminal program.
LINUX	
XTERMR6	
SCO	
ESCN	
VT400	

Default setting: VT100

2.6.2.2.12 Redirection After BIOS POST

SETTING	DESCRIPTION
Always Enable	Use this setting to specify that console redirection is always enabled for legacy OS.
BootLoader	User this setting to specify that console redirection is disabled for legacy OS.

Default setting: Always Enable

2.6.3 Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

The following functions control the presence and content of the ACPI serial port redirection table (SPCR). This table is mainly used by the Windows server variants to provide Windows Emergency Management Services (EMS). This functionality is totally independent from serial redirection of other console output.

2.6.3.1 Console Redirection

SETTING	DESCRIPTION
Disabled	Use this setting to prevent the system from adding the SPCR table to the ACPI tables.
Enabled	Use this setting to add the SPCR table to the ACPI tables. The OS can further use the information provided for serial redirection services.

Default setting: Disabled



2.6.3.2 Console Redirection Settings

This screen provides information about functions for specifying the Console Redirection configuration settings for the Out-of-Band Management / Windows Emergency Management Services (EMS).

Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.

Main

Serial Port for Out-of-Band Management Console Redirection Settings		
Out-of-Band Mgmt Port	COM0	
Terminal Type	[VT-UTF8]	
Bits per second	[115200]	
Flow Control	[None]	
Data Bits	8	
Parity	None	
Stop Bits	1	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.

2.6.3.2.1 Out-of-Band Mgmt Port

This function is used to select the serial port intended for use with Out-of-Band Management.

Note: This function is available only when the respective serial port is enabled.

SETTING	DESCRIPTION
COM0	Use this setting to specify that the serial port 0 is to be used with Out-of-Band Management
COM1	Use this setting to specify that the serial port 1 is to be used with Out-of-Band Management

Default setting: COM0

2.6.3.2.2 Terminal Type

SETTING	DESCRIPTION
VT100	Use one of these settings to select the terminal type to be emulated.
VT100+	
VT-UTF8	
ANSI	

Default setting: VT-UTF8



2.6.3.2.3 Bits per second

SETTING	DESCRIPTION
9600	Use one of these settings to select the baud rate of the serial port.
19200	
57600	
115200	

Default setting: 115200

2.6.3.2.4 Flow Control

SETTING	DESCRIPTION
None	Use one of these settings to specify the type of flow control to be used for this serial port.
Hardware RTS/CTS	
Software Xon/Xoff	

Default setting: None

2.6.3.2.5 Data Bits

This is a display-only function providing information about the frame width for the Out-of-Band Management.

2.6.3.2.6 Parity

This is a display-only function providing information about the parity for Out-of-Band Management.

2.6.3.2.7 Stop Bits

This is a display-only function providing information about the number of stop bits for Out-of-Band Management.



2.7 Intel ICC

This screen provides functions for specifying the spread spectrum configuration in the Intel ICC.

Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.

Main

DIV-2S BCLK, DMI, PEG, PCIe, PCI33, SATA, USB3 Maximum supported frequency 100.00 MHz Minimum supported frequency 100.00 MHz Current frequency 100.00 MHz Supported SSC modes Down Current SSC mode Down New SSC Mode [down] Maximum supported SSC 0.50% Current SSC % 0.50% New SSC spread percentage 50 ▶ Apply settings immediately ▶ Apply settings permanently after reboot	→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
--	--

Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.

2.7.1 Maximum supported frequency/Minimum supported frequency/Current frequency/Supported SSC modes/Current SSC mode/Maximum supported SSC/Current SSC %

These are display-only functions providing general information about the ICC generated clocks.

2.7.2 New SSC Mode

This function specifies the requested Spread Spectrum Clock (SSC) mode.

Default setting: down

Note: Please leave this function at the default setting to ensure reliable system operation. Changing the setting may lead to system instability.

2.7.3 New SSC spread percentage

Use this function to specify the requested Spread Spectrum Clock (SSC) in 0.01% increments.

SETTING	DESCRIPTION
0...50	Use this setting to select the new SSC value.

Default setting: 50



2.7.4 Apply settings immediately

Select this function and press “Enter” to make the setting of the new SSC spread percentage immediately valid. The changes will not remain valid after reboot. Making changes to this function may cause system instability and spontaneous restart.

2.7.5 Apply settings permanently after reboot

Select this function and press “Enter” to make the setting of the new SSC spread percentage permanently valid after reboot.

2.8 System Language

SETTING	DESCRIPTION
English	Use this function to select the system language. Currently, only English is supported.

2.9 System Date

SETTING	DESCRIPTION
<WD MM/DD/YYYY>	Use this function to change the system date. Select System Date using the Up and Down <Arrow> keys. Enter the new values through the keyboard or press +/- to increment/decrement values. Use “Tab” to switch between date elements.

2.10 System Time

SETTING	DESCRIPTION
<HH:MM:SS>	Use this function to change the system time. Select System Time using the Up and Down <Arrow> keys. Enter the new values through the keyboard or press +/- to increment/decrement values. Use “Tab” to switch between time elements.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as 17:30:00.

2.11 Access Level

This function provides display-only information concerning the uEFI BIOS Setup accessibility for the current Setup session. The access level is either “Administrator” or “User”.



Chapter **3**

Boot Setup



This page has been intentionally left blank.





3. Boot Setup

Select the Boot tab to enter the Boot Setup screen. This screen lists the sub-screens for boot configuration and boot device priority.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Boot

<p>Boot Configuration</p> <p>Setup Prompt Timeout 1</p> <p>Bootup NumLock State [On]</p> <p>Quiet Boot [Disabled]</p> <p>Fast Boot [Disabled]</p> <p>CSM16 Module Version 07.68</p> <p>GateA20 Active [Upon Request]</p> <p>Option ROM Messages [Force BIOS]</p> <p>Interrupt 19 Capture [Disabled]</p> <p>Boot Option Priorities</p> <p>Boot Option #1 [Built-in EFI Shell]</p> <p>Boot Option #2 [SanDisk uSSD 5000 ...]</p> <p>Boot Option #3 [P0: ...]</p> <p>Boot Option #4 [P1: ...]</p> <p>Hard Drive BBS Priorities</p> <p>Network Device BBS Priorities</p> <p>CD/DVD ROM Drive BBS Priorities</p> <p>Floppy Drive BBS Priorities</p> <p>BEV Device BBS Priorities</p>	<p>→←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Exit</p> <p>ESC: Exit</p>
---	---

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

3.1 Boot Configuration

3.1.1 Setup Prompt Timeout

This integer function is used to set an additional time the POST should wait for the operator to press the key to enter setup. The time is entered in seconds.

SETTING	DESCRIPTION
1 ⋮ 65535	Use one of these settings to specify the setup prompt timeout.

Default setting: 1



3.1.2 Bootup NumLock State

This function is used to set the state of the keyboard's numlock function after POST.

SETTING	DESCRIPTION
On	Use this setting to switch on the keyboard's numlock function after POST.
Off	Use this setting to switch off the keyboard's numlock function after POST.

Default setting: On

3.1.3 Quiet Boot

This function is used to display either POST output messages or a splash screen during boot-up.

SETTING	DESCRIPTION
Disabled	Use this setting to display POST output messages during boot-up.
Enabled	Use this setting to display a splash screen during boot-up.

Default setting: Disabled

3.1.4 Fast Boot

This function is used to enable or disable boot with initialization of a minimal set of devices required to launch active boot option..

SETTING	DESCRIPTION
Disabled	Use this setting to disable fast boot.
Enabled	Use this setting to enable fast boot.

Default setting: Disabled

3.1.5 CSM16 Module Version

This function provides display-only information concerning the CSM Module and is intended for internal use only.

3.1.6 GateA20 Active

This function is used to enable or disable GateA20.

SETTING	DESCRIPTION
Upon Request	Use this setting to disable GA20 in the uEFI BIOS.
Always	Use this setting to prevent the system from disabling GA20.

Default setting: Upon Request



3.1.7 Option ROM Messages

This function is used to control the messages of the loaded PCI option ROMs.

SETTING	DESCRIPTION
Force BIOS	Use this setting to force to a BIOS-compatible output. This will show the option ROM messages.
Keep Current	Use this setting to keep the current video mode. This will suppress option ROM messages. Option ROMs requiring interactive inputs may not work properly in this mode.

Default setting: Force BIOS

3.1.8 Interrupt 19 Capture

This function is used to specify if legacy PCI option ROMs are allowed to capture software interrupt 19h.

SETTING	DESCRIPTION
Disabled	Use this setting to prevent legacy PCI option ROMs from capturing software interrupt 19h.
Enabled	Use this setting to allow legacy PCI option ROMs to capture software interrupt 19h.

Default setting: Disabled

3.2 Boot Option Priorities

3.2.1 Boot Option #1..4

These functions are used to form the boot order and are dynamically generated. They represent either a legacy BBS (BIOS Boot Specification) class of devices or a native uEFI boot entry. Press Return on each option to select the BBS class / uEFI boot entry desired.

3.2.2 Hard Drive/Network Device/CD/DVD ROM Drive/Floppy Drive/BEV Device BBS Priorities

These functions lead to sub-menus that allow configuring the boot order for a specific device class. These options are visible only if at least one device for this class is present. These functions are dynamically generated.



This page has been intentionally left blank.





Chapter **4**

Security Setup



This page has been intentionally left blank.





4. Security Setup

Select the Security tab to enter the Security Setup screen. This screen provides information about the passwords and functions for specifying the security settings.

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.

Security

<p>Password Description</p> <p>If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.</p> <p>If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.</p> <p>The password length must be in the following range:</p> <table style="width: 100%; border: none;"> <tr> <td style="padding-left: 20px;">Minimum length</td> <td style="text-align: right;">3</td> </tr> <tr> <td style="padding-left: 20px;">Maximum length</td> <td style="text-align: right;">20</td> </tr> </table> <p style="margin-top: 20px;">Administrator Password</p> <p style="margin-top: 5px;">User Password</p> <p style="margin-top: 20px;">HDD Security Configur</p> <p style="margin-top: 5px;">HDD 0:ST9120822SB</p>	Minimum length	3	Maximum length	20	<p>→←: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Exit</p> <p>ESC: Exit</p>
Minimum length	3				
Maximum length	20				

Version 2.10.1208. Copyright (C) 2010 American Megatrends, Inc.

The following modes of security are provided:

SETTING	DESCRIPTION
No password is set	Booting the system as well as entering the Setup is unsecured.
Only Administrator password is set	Booting the system is unsecured. If no valid Administrator password is entered, only limited access to Setup is provided.
Only User password is set	The User password is required for booting the system as well as for entering the Setup menu. On every start-up, the user will be asked for the password.
Both User and Administrator passwords are set	Either the User or the Administrator password is required for booting the system as well as for entering the Setup menu. If the User password is entered here, limited access to the Setup is granted. Entering the Administrator password provides full access to all Setup entries.

Note: The CP6004-SA/-RA/-RC/CP6004X-SA provides no factory-set passwords.



4.1 Administrator Password

This function is used to set, change or delete the Administrator password. If there is already a password installed, the system asks for this first. To clear a password, simply enter nothing and acknowledge by pressing Return. To set a password, enter it twice and acknowledge by pressing Return.

Note: The password is case-sensitive.

4.2 User Password

This function is used to set, change or delete the User password. If there is already a password installed, the system asks for this first. To clear a password, simply enter nothing and acknowledge by pressing Return. To set a password, enter it twice and acknowledge by pressing Return.

Note: The password is case-sensitive.

4.3 HDD Security Configuration

This function is not fully supported on the CP6004-SA/-RA/-RC/CP6004X-SA.

Warning! Before using this function, contact Kontron for assistance. Failure to comply with the instruction above may result in an irreparable disk lockout.

4.4 Remember the Password

It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords may lead to being completely locked out of the system. Booting may not be possible, and in worst case the uEFI BIOS Setup program will also not be accessible.

If the system cannot be booted because neither the uEFI BIOS User password nor the Administrator password are known, refer to the CP6004-SA User Guide / CP6004X-SA User Guide / CP6004-RA/-RC User Guide, Chapter 4.1, for information about clearing the uEFI BIOS settings, or contact Kontron for further assistance.



Chapter

5

Save & Exit

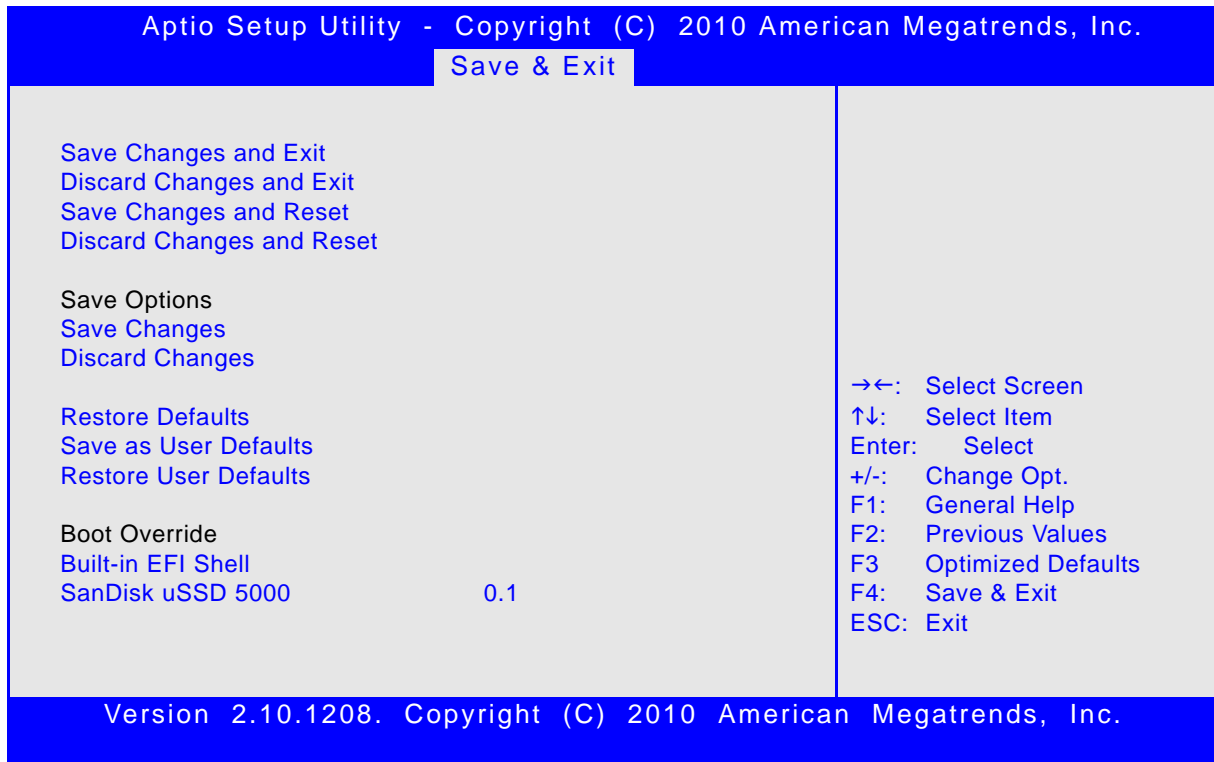


This page has been intentionally left blank.



5. Save & Exit

Select the Save & Exit tab to enter the Save & Exit menu screen. This screen provides functions for handling changes made to the uEFI BIOS settings and the exiting of the Setup program.



5.1 Save Changes and Exit

This function is used to save all changes made within the Setup to flash. This function continues the boot process as long as no option was altered that requires a reboot.

Note: The Setup will ask for confirmation prior to executing this command.

5.2 Discard Changes and Exit

This function is used to discard all changes made within the Setup. This function continues the boot process.

Note: The Setup will ask for confirmation prior to executing this command.

5.3 Save Changes and Reset

This function is used to save all changes made within the Setup to flash. This function performs a reboot afterwards.

Note: The Setup will ask for confirmation prior to executing this command.



5.4 Discard Changes and Reset

This function is used to discard all changes made within the Setup. This function performs a reboot afterwards.

Note: The Setup will ask for confirmation prior to executing this command.

5.5 Save Changes (Save Options)

This function is used to save all changes made within the Setup to flash. This function returns to Setup.

Note: The Setup will ask for confirmation prior to executing this command.

5.6 Discard Changes (Save Options)

This function is used to discard all changes made within the Setup. This function returns to Setup.

Note: The Setup will ask for confirmation prior to executing this command.

5.7 Restore Defaults (Save Options)

This function is used to restore all tokens to factory default.

Note: The Setup will ask for confirmation prior to executing this command.

5.8 Save as User Defaults (Save Options)

This function is used to save all current settings as user default. The current setup state can later be restored using Restore User Defaults.

Note: The Setup will ask for confirmation prior to executing this command.

5.9 Restore User Defaults (Save Options)

This function is used to restore all tokens to settings previously stored by Save as User Defaults.

Note: The Setup will ask for confirmation prior to executing this command.

5.10 Boot Override

This group of functions includes a list of tokens, each of them corresponding to one device within the boot order. Select a drive to immediately boot that device regardless of the current boot order. If booting to uEFI Shell this way, an exit from the shell returns to Setup.



Chapter

6

The uEFI Shell



This page has been intentionally left blank.





6. The uEFI Shell

The Kontron uEFI BIOS features a built-in and enhanced version of the uEFI Shell. For a detailed description of the available standard shell scripting refer to the EFI Shell User's Guide. For a detailed description of the available standard shell commands, refer to the Shell Command Manual 1.0. Both documents can be downloaded from the EFI and Framework Open Source Community homepage (<https://efi-shell.tianocore.org>) under the "Documents and Files" section.

Please note that not all shell commands described in the Shell Command Manual 1.0 are provided by the Kontron uEFI BIOS.

6.1 Introduction, Basic Operation

The uEFI Shell forms an entry into the uEFI boot order and is the first boot option by default. It is simply started by putting the uEFI Shell first in boot and running the board as usual.

6.1.1 Shell Startup

If the shell is executed, it displays its signon message followed by a list of detected devices. The output produced by the device mapping table can vary depending on the board's configuration.

```
EFI Shell version 2.00 [4.631]
Current running mode 1.1.2
Device mapping table
fs0      :Removable HardDisk - Alias hd33b0b0b blk0
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
fs1      :Removable BlockDevice - Alias f33b0c0 blk1
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(2, 0)
blk0     :Removable HardDisk - Alias hd33b0b0b fs0
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig17731773)
blk1     :Removable BlockDevice - Alias f33b0c0 fs1
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(2, 0)
blk2     :HardDisk - Alias (null)
          Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)/HD(Part1,SigC811D18D)
blk3     :BlockDevice - Alias (null)
          Acpi(PNP0A03,0)/Pci(1F|2)/Ata(Primary,Master)
blk4     :Removable BlockDevice - Alias (null)
          Acpi(PNP0A03,0)/Pci(1D|7)/Usb(1, 0)/Usb(1, 0)
```

Press the ESC key within 5 seconds to skip startup.nsh, and any other key to continue.

If the ESC key is pressed before the 5-second timeout has elapsed, the shell prompt is shown:

```
Shell>
```



6.2 Kontron Shell Commands

The Kontron uEFI implementation provides the following additional commands related to the specific HW features of the Kontron system:

- **kBiosRevision**
- **kboardconfig**
- **kboardinfo**
- **kboot**
- **kbootnsh**
- **kclearnvram**
- **kflash**
- **kipmi**
- **kmkramdisk**
- **kpassword**
- **kresetconfig**
- **kwdt**

The following chapters provide information concerning these Kontron-specific commands. Where “RESPONSE” information is provided in “USAGE”, the value indicated in brackets is the currently selected setting. Where “SETTINGS” information is provided, the value indicated in brackets is the default setting. The uEFI Shell commands are case-sensitive.



6.2.1 kBiosRevision uEFI Shell Command

kBiosRevision

FUNCTION:	Get uEFI BIOS revision
SYNTAX:	<pre>kbiosrevision [-?] [[-lt] [-eq] [-gt] <number>]</pre> <p>where:</p> <ul style="list-style-type: none"> -? Show help -lt Check if current uEFI BIOS revision is less than <number> -eq Check if current uEFI BIOS revision is equal to <number> -gt Check if current uEFI BIOS revision is greater than <number> <p><number> (uEFI BIOS) revision number</p>
DESCRIPTION:	<p>The kBiosRevision command is used to display the current uEFI BIOS revision.</p> <p>In scripting environments it can be used to perform checks against a uEFI BIOS revision number provided in the script.</p>
USAGE:	<p>Display current uEFI BIOS revision:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>Shell> kbiosrevision BIOS revision: 14</pre> <p>Check if current uEFI BIOS revision is equal to R14: (used within uEFI shell script)</p> <pre>kbiosrevision -eq 14 if not %lasterror% == 0 then echo "NOT R14 , need to update" goto _update else "EFI R14 found" endif</pre>

6.2.2 kboardconfig uEFI Shell Command

kboardconfig

FUNCTION:	Configure the non-volatile board settings																
SYNTAX:	<p>kboardconfig [-?][-b][-nc] <option> <parameter></p> <p>where:</p> <ul style="list-style-type: none"> ? Used to show HELP -b Used to invoke page break in the display output -nc Used to disable color <option> Used to select option <parameter> Used to specify parameter for option selected <p>The command notation above indicates only the possible modifiers and not the command's syntax logic.</p> <p>There are eight defined variations of this command:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">kboardconfig</td> <td style="padding: 2px;">lists options and their current status</td> </tr> <tr> <td style="padding: 2px;">kboardconfig -b</td> <td style="padding: 2px;">lists options, their current status, and invokes page breaks in the display output</td> </tr> <tr> <td style="padding: 2px;">kboardconfig -nc</td> <td style="padding: 2px;">lists options, their current status, and disables color in the display output</td> </tr> <tr> <td style="padding: 2px;">kboardconfig -?</td> <td style="padding: 2px;">provides HELP information</td> </tr> <tr> <td style="padding: 2px;">kboardconfig -? -b</td> <td style="padding: 2px;">provides HELP information and invokes page breaks in the display output</td> </tr> <tr> <td style="padding: 2px;">kboardconfig <option></td> <td style="padding: 2px;">provides HELP for option specified and the current status of the option</td> </tr> <tr> <td style="padding: 2px;">kboardconfig <option> -nc</td> <td style="padding: 2px;">provides HELP for option specified, the current status of the option, and disables color in display output</td> </tr> <tr> <td style="padding: 2px;">kboardconfig <option> <parameter></td> <td style="padding: 2px;">sets the <parameter> to be used with the <option> specified</td> </tr> </table>	kboardconfig	lists options and their current status	kboardconfig -b	lists options, their current status, and invokes page breaks in the display output	kboardconfig -nc	lists options, their current status, and disables color in the display output	kboardconfig -?	provides HELP information	kboardconfig -? -b	provides HELP information and invokes page breaks in the display output	kboardconfig <option>	provides HELP for option specified and the current status of the option	kboardconfig <option> -nc	provides HELP for option specified, the current status of the option, and disables color in display output	kboardconfig <option> <parameter>	sets the <parameter> to be used with the <option> specified
kboardconfig	lists options and their current status																
kboardconfig -b	lists options, their current status, and invokes page breaks in the display output																
kboardconfig -nc	lists options, their current status, and disables color in the display output																
kboardconfig -?	provides HELP information																
kboardconfig -? -b	provides HELP information and invokes page breaks in the display output																
kboardconfig <option>	provides HELP for option specified and the current status of the option																
kboardconfig <option> -nc	provides HELP for option specified, the current status of the option, and disables color in display output																
kboardconfig <option> <parameter>	sets the <parameter> to be used with the <option> specified																
DESCRIPTION:	The kboardconfig command is used to configure non-volatile board settings. For information on default settings, refer to Chapter 5.7, Restore Defaults, and Chapter 6.2.6, kclearnvram uEFI Shell Command.																

kboardconfig (continued)

```
USAGE: Command: kboardconfig  
Shows all options and their current parameter setting.  
COMMAND / RESPONSE EXAMPLE:  
Shell> kboardconfig  
Pxe -> disabled  
StorageOprom -> enabled  
PrimaryDisplay -> auto  
Vga -> front  
SataMode -> ahci  
Sata0Speed -> Gen3  
Sata1Speed -> Gen3  
Sata2Speed -> Gen2  
Sata3Speed -> Gen2  
Sata4Speed -> Gen2  
Sata5Speed -> Gen2  
Sata0Hotplug -> disabled  
Sata1Hotplug -> disabled  
Sata2Hotplug -> disabled  
Sata3Hotplug -> disabled  
Sata4Hotplug -> disabled  
Sata5Hotplug -> disabled  
WrProtSata -> disabled  
WrProtEeprom -> disabled  
WrProtSpi -> disabled  
IntelVT -> enabled  
IntelHT -> enabled  
SpeedStep -> enabled  
CpuTurbo -> enabled  
C3State -> disabled  
C6State -> disabled  
C7State -> enabled  
PciCfgDelay -> disabled
```

**kboardconfig (continued)**

USAGE: Command: **kboardconfig -?**
Shows HELP information for the kboardconfig command.

COMMAND / RESPONSE EXAMPLE:
`Shell> kboardconfig -?`
Control nonvolatile board settings

Example: `kboardconfig <option> <parameter>`

Show all options and their current status:
`kboardconfig`

Show help:
`kboardconfig -?`

Show all options and their current status with page break:
`kboardconfig -b`

Show all options and their current status without color:
`kboardconfig -nc`

Show help and status for a single option:
`kboardconfig <option>`
`kboardconfig -nc <option>`

Change parameter for an option:
`kboardconfig <option> <parameter>`

**kboardconfig (continued)**

Command: **kboardconfig <option>**

Show help and status for a single option:

COMMAND / RESPONSE EXAMPLE (CP6004-SA/-RA/-RC):

```
Shell> kboardconfig Pxe
```

Pxe:

PXE boot device

Available parameters: [disabled], all, gbe_a, gbe_b, rear_a, rear_b, gbe_e

In this case “disabled” is the current setting.

COMMAND / RESPONSE EXAMPLE (CP6004X-SA):

```
Shell> kboardconfig Pxe
```

Pxe:

PXE boot device

Available parameters: [disabled], all, gbe_a, gbe_b, rear_a, rear_b, gbe_e, 10gbe_1, 10gbe_2

In this case “disabled” is the current setting.

USAGE:

Command: **kboardconfig <option> <parameter>**

Set option “Pxe” to parameter “all”:

COMMAND / RESPONSE EXAMPLE:

```
Shell> kboardconfig Pxe all
```

The response for “kboardconfig” with <option> and <parameter> is the display of a status line indicating the performance status of the command and one or more lines providing further information related to the command performance.

kboardconfig (continued)

OPTIONS: The listing below provides an overview of the possible options and a short description of their functionality.

To view all of the possible parameters for a given option, use the command "kboardconfig <option>".

OPTION	DESCRIPTION
a11:	Try all Ethernet devices round robin for PXE boot
Pxe	Used to select a PXE boot device
gbe_a:	CP6004-SA/CP6004X-SA: Gigabit Ethernet available on the front panel GbE A port.
gbe_a:	CP6004-RA: Gigabit Ethernet available on the front panel GbE A port or on the rear I/O LPc port
gbe_a:	CP6004-RC: Gigabit Ethernet available on the rear I/O LPc port
gbe_b:	CP6004-SA/CP6004X-SA: Gigabit Ethernet available on the front panel GbE B port.
gbe_b:	CP6004-RA: Gigabit Ethernet available on the front panel GbE B port or on the rear I/O LPd port
gbe_b:	CP6004-RC: Gigabit Ethernet available on the rear I/O LPd port
gbe_e:	CP6004-SA/CP6004X-SA: Gigabit Ethernet available on the front panel GbE E port.
gbe_e:	CP6004-RA: Gigabit Ethernet available on the front panel GbE C port.
gbe_e:	CP6004-RC: function not supported
rear_a, rear_b:	Ethernet ports PICMG 2.16 LPa and LPb available on the rear I/O.
10gbe_1, 10gbe_2:	10 Gigabit Ethernet ports routed to the backplane (only on CP6004X-SA)
	10gbe_1 corresponds to port 0 on the Intel® 82599 controller (10GBE2 high-speed serial rear I/O port)
	10gbe_2 corresponds to port 1 on the Intel® 82599 controller (10GBE1 high-speed serial rear I/O port)
StorageOprom	Used to launch the Storage PCI OPROM When disabled it includes the onboard RAID option ROM.

kboardconfig (continued)

OPTIONS:		
	PrimaryDisplay	Used to select the primary display device auto : Automatically detect primary display device igfx : Use internal graphics, if enabled peg : Try to use video on the PCIe graphics port, if present pci : Try to use video on the PCI(e) bus first
	Vga	Used to select the VGA port configuration (CP6004-SA/CP6004X-SA) Note: This function is not relevant on the CP6004-RA/-RC as the VGA port is statically routed to rear I/O.
	SataMode	Used to select the operational configuration for the SATA controller ide : SATA ports operate as two IDE controllers ahci : SATA ports operate as one 6-port AHCI controller raid : SATA ports form a RAID device Note : For this command to take effect, the system must be re-booted. During the bootup, it is possible to select a menu to specify the desired RAID configuration. Entry to this menu is achieved by pressing "Ctrl + I" when requested during the bootup.
	Sata0Speed	Indicates maximum speed supported by SATA port 0 (on the SATA Flash module) Available parameters for SATA0Speed and SATA1Speed: Gen1 (SATA 1.5 Gb/s), Gen2 (SATA 3.0 Gb/s), Gen3 (SATA 6.0 Gb/s)
	Sata1Speed	Indicates maximum speed supported by SATA port 1 (onboard SATA connector J14) For available parameters, refer to SATA0Speed.
	Sata2Speed	Indicates maximum speed supported by SATA port 2 (SATA port on the CPCI rear I/O connector J5) Available parameters for SATA2Speed to SATA5Speed: Gen1 (SATA 1.5 Gb/s), Gen2 (SATA 3.0 Gb/s)
	Sata3Speed	Indicates maximum speed supported by SATA port 3 (SATA port on the CPCI rear I/O connector J5) For available parameters, refer to SATA2Speed.
	Sata4Speed	Indicates maximum speed supported by SATA port 4 (SATA port on the CPCI rear I/O connector J5) For available parameters, refer to SATA2Speed.

kboardconfig (continued)

OPTIONS:	Sata5Speed	Indicates maximum speed supported by SATA port 5 (SATA port on the CPCI rear I/O connector J5) For available parameters, refer to SATA2Speed.
	Sata0Hotplug:	Enable hotplug for SATA port 0 (on the SATA Flash module)
	Sata1Hotplug:	Enable hotplug for SATA port 1 (onboard SATA connector J14)
	Sata2Hotplug:	Enable hotplug for SATA port 2 (SATA port on the CPCI rear I/O connector J5)
	Sata3Hotplug:	Enable hotplug for SATA port 3 (SATA port on the CPCI rear I/O connector J5)
	Sata4Hotplug:	Enable hotplug for SATA port (SATA port on the CPCI rear I/O connector J5)
	Sata5Hotplug:	Enable hotplug for SATA port (SATA port on the CPCI rear I/O connector J5)
	WrProtSata:	Used to select onboard SATA flash write protection If enabled, the onboard SATA flash is write-protected after POST. OS needs to be prepared to work with write-protected flash. For further information, refer to the operating system's documentation. Note: Please contact Kontron before using this function.
	WrProtEeprom:	Used to select onboard system EEPROM write protection If enabled, the system EEPROM is write-protected after POST.
	WrProtSpi	Used to select onboard SPI boot flash write protection If enabled, both of the onboard SPI boot flashes are write-protected after POST.
	IntelVT	Used to enable Intel® VT-x Virtualization Technology
	IntelHT	Used to enable Intel® Hyper-Threading Technology
	SpeedStep	Used to enable Intel® SpeedStep®
	CpuTurbo	Used to enable CPU turbo mode
	C3State	Used to enable CPU C3-State report to OS
C6State	Used to enable CPU C6-State report to OS	
C7State	Used to enable CPU C7-State report to OS	
PciCfgDelay	Used to set a delay for PCI config cycles	



6.2.3 kboardinfo uEFI Shell Command

kboardinfo

FUNCTION:	Show board identification data
SYNTAX:	<code>kboardinfo</code>
DESCRIPTION:	The kboardinfo command shows a summary of board-specific identification data. It is especially useful for support queries because it contains this data in a concentrated form.
USAGE:	<p>Show board identification data</p> <p>COMMAND / RESPONSE EXAMPLE (CP6004-SA):</p> <pre>Shell> kboardinfo KOMaOEMF rev.: 4 Board ID: 0xB3D0 Hardware rev.: 0x0 Logic rev.: 0x1 Boot flash: Standard SPI boot flash In system slot: No Geographic address: 8 Material number: Hardware index: Serial number: EFI article name: SK-EFI-B3D01 EFI material number: 1052-6900 EFI index: 14, standard EFI bulid time: 09:50:41 EFI build date: 01/09/2013 CPU rev.: 0x9 Chipset rev.: 0x4 Microcode: 0x12 CPU ID: 0x306A9 CPU Branding: Intel(R) Core(TM) i7-3615QE CPU @ 2.30 GHz RIO Module: present ME firmware rev: 8.1.20.1336 VBIOS rev.: 2137</pre>

**kboardinfo (continued)**

```
USAGE: COMMAND / RESPONSE EXAMPLE (CP6004-RA):  
Shell> kboardinfo  
KOMaOEMF rev.:      4  
Board ID:           0xB3D9  
Hardware rev.:      0x0  
Logic rev.:         0x4  
Boot flash:         Standard SPI boot flash  
In system slot:     No  
Geographic address: 8  
Material number:  
Hardware index:  
Serial number:  
EFI article name:   SK-EFI-B3D01  
EFI material number: 1052-6900  
EFI index:          14, standard  
EFI bulid time:     09:50:41  
EFI build date:     01/09/2013  
CPU rev.:           0x9  
Chipset rev.:       0x4  
Microcode:          0x12  
CPU ID:             0x306A9  
CPU Branding:       Intel(R) Core(TM) i7-3612QE  
                    CPU @ 2.10 GHz  
RIO Module:         present  
ME firmware rev:    8.1.20.1336  
VBIOS rev.:         2137
```

**kboardinfo (continued)**

```
USAGE: COMMAND / RESPONSE EXAMPLE (CP6004-RC):  
Shell> kboardinfo  
KOMaOEMF rev.:      4  
Board ID:           0xB3D8  
Hardware rev.:     0x0  
Logic rev.:        0x4  
Boot flash:        Standard SPI boot flash  
In system slot:    No  
Geographic address: 8  
Material number:  
Hardware index:  
Serial number:  
EFI article name:  SK-EFI-B3D01  
EFI material number: 1052-6900  
EFI index:         14, standard  
EFI bulid time:    09:50:41  
EFI build date:    01/09/2013  
CPU rev.:          0x9  
Chipset rev.:      0x4  
Microcode:         0x12  
CPU ID:            0x306A9  
CPU Branding:      Intel(R) Core(TM) i7-3555LE  
                   CPU @ 2.50 GHz  
RIO Module:        present  
ME firmware rev:   8.1.20.1336  
VBIOS rev.:        2137
```

**kboardinfo (continued)**

```
USAGE: COMMAND / RESPONSE EXAMPLE (CP6004X-SA):  
Shell> kboardinfo  
KOMaOEMF rev.:      4  
Board ID:           0xB3E8  
Hardware rev.:      0x0  
Logic rev.:         0x1  
Boot flash:         Standard SPI boot flash  
In system slot:     No  
Geographic address: 8  
Material number:  
Hardware index:  
Serial number:  
EFI article name:   SK-EFI-B3D01  
EFI material number: 1052-6900  
EFI index:          14, standard  
EFI bulid time:     09:50:41  
EFI build date:     01/09/2013  
CPU rev.:           0x9  
Chipset rev.:       0x4  
Microcode:          0x12  
CPU ID:             0x306A9  
CPU Branding:       Intel(R) Core(TM) i7-3615QE  
                    CPU @ 2.30 GHz  
RIO Module:         present  
ME firmware rev:    8.1.20.1336  
VBIOS rev.:         2137
```

**kboardinfo (continued)**

USAGE:	KOMaOEMF rev.:	Revision of KOMaOEMF protocol
	Board ID:	Kontron board identification value
	Hardware rev.:	Hardware revision of this board
	Logic rev.:	Logic revision of this board
	Boot flash:	Current boot flash: either "Standard SPI boot flash" or "Recovery SPI boot flash"
	In system slot:	Indicates whether the board is installed in the system slot.
	Geographic Address:	Geographic address of the cPCI backplane slot the board is currently plugged into
	Material number:	Kontron hardware reference number
	Hardware index:	Kontron hardware index
	Serial number:	This board's unique serial number
	EFI article name:	Kontron uEFI reference name
	EFI material number:	Kontron uEFI reference number
	EFI index:	Version of this uEFI BIOS
	EFI build time:	Build time of this uEFI BIOS
	EFI build date:	Build date of this uEFI BIOS
	CPU rev.:	Chip revision of the CPU
	Chipset rev.:	Chip revision of the Chipset
	Microcode:	Currently loaded microcode
	CPU ID:	CPU ID
	CPU Branding:	CPU identification string
RIO Module:	RIO module present / not present	
ME firmware rev:	Intel® Management Engine (ME) firmware revision	
VBIOS rev.:	Video BIOS revision	



6.2.4 kboot uEFI Shell Command

kboot

FUNCTION:	Boot a legacy OS Not to be used for uEFI BootLoaders!
SYNTAX:	<pre>kboot [-? -d -p -p <path> -n <name> -t <type>]</pre> <p>where:</p> <ul style="list-style-type: none"> ? Show online help -d Boot default order -p <path> Specify the path to the device to boot from -n <name> Specify the device name to boot from -t <type> Specify the device type to boot from <p>Available types are:</p> <ul style="list-style-type: none"> floppy harddrive cdrom network usb-floppy usb-harddrive usb-cdrom
DESCRIPTION:	The kboot command boots a legacy OS. Boot device can be selected in a very flexible way. If the requested device is not present, boot returns to shell. The kboot command cannot boot native uEFI-aware operating systems. But since these are bootable from shell by calling their bootloader, this is not necessary either. If a requested device is present but not bootable, uEFI continues to boot with the next bootable device in the boot order.
USAGE:	<p>Show all connected devices:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>fs0:\> kboot _____ BBS TABLE 00002 network "IBA GE Slot 0100 v1300" 00003 network "IBA GE Slot 0101 v1300" 00004 network "IBA GE Slot 0200 v1300" 00005 network "IBA GE Slot 0201 v1300" 00002 usb-harddrive "SanDisk uSSD 5000 0.1" Device path: Acpi(PNP0A03,0)/Pci(1A 7)/Usb(1,0) 0001 usb-harddrive "KingstonDataTraveler 2.04.10" Device path: Acpi(PNP0A03,0)/Pci(1D 7)/Usb(1,0)</pre> <p>Boot from device containing the string "Kingston":</p> <pre>fs0:\> kboot -n Kingston</pre> <p>Boot from the first device found that is of type floppy:</p> <pre>fs0:\> kboot -t floppy</pre>



6.2.5 kbootnsh uEFI Shell Command

kbootnsh

FUNCTION:	Manage the startup script stored in the flash
SYNTAX:	<pre>kbootnsh [-b][-? -g <filename> -p <filename> -d]</pre> <p>where:</p> <ul style="list-style-type: none"> -b Display output page by page -? Show online help -g <filename> Store the current boot script to disk. If there is no physical disk drive present, the kmkramdisk command may be used. -p <filename> Store the shell script pointed to by filename to flash. Note: The shell script cannot be larger than 400 bytes. -d Delete the current startup script from flash.
DESCRIPTION:	The kbootnsh command manages the flash stored startup script. If the shell is launched by the boot process, it executes a shell script stored in the flash. If the shell script terminates, the shell executes a kboot -d command to continue the boot process. However, the shell script can of course contain any other boot command.
USAGE:	<p>Get current startup script to file named boot.nsh</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>shell> kbootnsh -g boot.nsh</pre> <p>Store file named boot.nsh to flash:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>shell> kbootnsh -p boot.nsh</pre> <p>Delete startup script:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>shell> kbootnsh -d</pre>

6.2.6 kclearnvram uEFI Shell Command

kclearnvram

FUNCTION:	Clear the NVRAM to restore the system's default settings
SYNTAX:	<pre>kclearnvram</pre> <p>No parameters required. For safety reasons this command must be confirmed by pressing "c".</p>
DESCRIPTION:	The kclearnvram command allows to clear the system NVRAM. Since all uEFI settings are stored inside the NVRAM, the default settings are loaded afterwards.



6.2.7 kflash uEFI Shell Command

kflash

FUNCTION:	Manage uEFI BIOS update
SYNTAX:	<p>kflash [-p -i -s -c -h -?] [-f] [-r] [file]</p> <p>Operation mode:</p> <ul style="list-style-type: none"> -p Program flash -i Show information string and check CRC -s Save current ROM image to file -c Clone flash content to second flash -h Show this help -? Show online help <p>file uEFI BIOS binary file</p> <p>Options:</p> <ul style="list-style-type: none"> -f Force write <p>Expert options: Not recommended for standard use</p> <ul style="list-style-type: none"> -r Raw image mode (.bin, .rom) -q Silent mode No user interaction needed.
DESCRIPTION:	The kflash command is used to program and verify the flash banks holding the uEFI BIOS code. uEFI BIOS binary files must be available from connected mass storage devices, such as USB flash drive or harddisk.
USAGE:	<p>Get help: COMMAND / RESPONSE EXAMPLE: shell> kflash -?</p> <p>Get help: COMMAND / RESPONSE EXAMPLE: shell> kflash -h</p> <p>Program the uEFI BIOS into the standard SPI boot flash: COMMAND / RESPONSE EXAMPLE: shell> kflash -p BIOS_file.kf1 Note: This function will select and update the standard SPI boot flash regardless of the DIP switch setting for boot selection.</p> <p>Copy the currently running uEFI BIOS into the inactive SPI boot flash: COMMAND / RESPONSE EXAMPLE: shell> kflash -c Note: Using this function will overwrite the inactive SPI boot flash. Failures during the process will make the inactive SPI boot flash invalid. In such cases, please execute the function again until the process completes successfully.</p>



6.2.8 kipmi uEFI Shell Command

kipmi

FUNCTION:	Read or configure available MMC parameters
SYNTAX:	<pre>kipmi [-? -b parameters]</pre> <p>where:</p> <ul style="list-style-type: none"> -? show online help -b display output page by page <p>parameters fru -- display fru data: [Fru Device ID] ipmb -- ipmb bus settings: ipmb [redundant / single] irq -- get / set KCS IRQ: irq [number] mode -- set ipmi controller mode: mode [bmc / smc] net -- display and change SOL network settings sel -- handle system event log sensor -- show sensor related information raw -- execute raw ipmi command rawsendmessage -- execute raw SendMessage ipmi cmd info -- show information about the device and firmware</p>
DESCRIPTION:	The kipmi command can read event logs or set the MMC IRQ configuration. This shell application can also be used to set up raw command to the MMC.
USAGE:	<p>Display fru data: COMMAND / RESPONSE EXAMPLE: <pre>shell> kipmi fru 0</pre></p> <p>Display ipmb bus settings: COMMAND / RESPONSE EXAMPLE: <pre>shell> kipmi ipmb</pre></p> <p>Change IRQ configuration: COMMAND / RESPONSE EXAMPLE: <pre>shell> kipmi irq 10</pre></p> <p>Show IRQ configuration: COMMAND / RESPONSE EXAMPLE: <pre>shell> kipmi irq</pre></p> <p>Set IPMI controller mode: COMMAND / RESPONSE EXAMPLE: <pre>shell> kipmi mode</pre></p>



kipmi (continued)

USAGE:	Set Serial-over-LAN I/O/SOL parameters: COMMAND / RESPONSE EXAMPLE: <code>Shell> kipmi net 1</code>
	Display system event log: COMMAND / RESPONSE EXAMPLE: <code>Shell> kipmi sel list</code>
	Show sensor related information: COMMAND / RESPONSE EXAMPLE: <code>Shell> kipmi sensor list</code>
	Execute raw command. Example: Get self-test results. COMMAND / RESPONSE EXAMPLE: <code>Shell> kipmi raw 0x06 0x00 0x04</code>
	Execute raw SendMessage command: COMMAND / RESPONSE EXAMPLE: <code>Shell> kipmi rawsendmessage 0x20 0x00 0x06 0x00 0x01</code>
SETTINGS:	<code>fru [<Fru device ID>]:</code> Displays FRU data Options: <code>Fru device ID:</code> Numeric FRU device ID. The FRU ID 0 is used by default if no FRU ID is entered.
	<code>ipmb:</code> Displays IPMB bus settings <code>ipmb redundant:</code> Switch IPMB bus to redundant mode <code>ipmb single:</code> Switch IPMB bus to single mode Note: The redundant mode is not available on the CP6004-SA/-RA/-RC/CP6004X-SA. Please leave this function at single mode.
	<code>irq <number>:</code> Display/Set the IRQ number of the KCS interface Options: <code>0:</code> KCS uses no IRQ <code>10:</code> KCS uses IRQ 10 <code>11:</code> KCS uses IRQ 11 The board must be reset for the settings to apply.
	<code>mode <mode>:</code> Display/Set the IPMI controller operating mode Options: <code>bmc:</code> IPMI controller operates in BMC mode (master) <code>smc:</code> IPMI controller operates in SMC mode (slave)
	<code>net:</code> Set IPMI-over-LAN (IOL) / Serial-over-LAN (SOL) parameters
	<code>sel:</code> Display system event log

**kipmi (continued)**

SETTINGS:	sensor list read: Show board sensor data Options: list: Display an overview of all available board sensors read: Display specific sensor data
	raw [<bytes> <...>]: Execute raw IPMI command Syntax: raw [NetFn] [LUN] [COMMAND] ...
	rawsendmessage [<bytes> <...>]: Execute raw SendMessage command Syntax: rawsendmessage [rsSa] [CHANNEL] [NetFn] [LUN] [COMMAND] ...
	info: Display IPMI firmware information

6.2.9 kmkramdisk uEFI Shell Command

kmkramdisk

FUNCTION:	Create RAMdisk drives
SYNTAX:	<pre>kmkramdisk [-? -s <size> <name>]</pre> <p>where:</p> <pre>-? show help</pre> <pre>-s <size> <name> create a RAMdisk of given size in Megabytes with the mount point name <name></pre>
DESCRIPTION:	<p>Creates a RAMdisk of variable size. Can be very useful to perform file operations when no real filesystem is connected to the system.</p> <p>Note: The RAMdisk loses its mount point name after all drives are remapped by the map -r command. The RAMdisk will then be enumerated as any other connected drive and gain a mount point name like "fs0". This is not a bug of the kmkramdisk command but a normal function of the uEFI framework.</p>
USAGE:	<p>Create RAMdisk:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>rd:\> kmkramdisk -s 5 myramdisk Device mapping table myramdisk :BlockDevice - Alias (null) VenMsg'(93B5F448-127A-4B29-B306- 5BE8AAC4826E) Success - Force file system to mount rd:\> myramdisk: myramdisk:\> echo testfile > testfile myramdisk:\> ls Directory of: myramdisk:\ 05/24/08 04:39a 22 testfile 1 File(s) 22 bytes 0 Dir(s)</pre>



6.2.10 kpassword uEFI Shell Command

kpassword

FUNCTION:	Control uEFI Setup and Shell passwords
SYNTAX:	<p>kpassword [-u -s -n -o]</p> <p>Call without parameters to get current password status</p> <p>Parameters:</p> <ul style="list-style-type: none"> -u Install or change User password -s Install or change Superuser password <p>Additional options for automated scripting:</p> <ul style="list-style-type: none"> -n New password to be set Use together with options “-u” or “-s”! -o Submit password if one is already set. Use together with options “-u” or “-s”! When used without the option “-n”, the password is cleared! <p>Note: Old passwords must be verified if set. Entering an empty password disables the password.</p>
DESCRIPTION:	The kpassword command is used to get and set the uEFI Shell and Setup passwords. Both User and Superuser (Administrator) passwords can be controlled.
USAGE:	<p>Control EFI setup and shell passwords</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>kpassword [-u -s -n -o] No password is installed! Enter new USER password --> Retype password --> Done.</pre>



6.2.11 kresetconfig uEFI Shell Command

kresetconfig

FUNCTION:	Control the board reset behavior
SYNTAX:	<pre>kresetconfig [-? <parameter>]</pre> <p>where:</p> <ul style="list-style-type: none"> -? Show help <parameter> pcislave [on off] <p>Controls if the board shall react on a CPCI backplane reset if it is used as slave board in a peripheral slot. It has no effect if the board is located within a CPCI master slot.</p> <p>Note: This parameter is volatile, and at next start is set to off.</p>
DESCRIPTION:	The kresetconfig command controls the board's reset behavior.
USAGE:	<p>Enable CPCI backplane reset:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>Shell> kresetconfig pcislave on Reset from system master is enabled</pre> <p>Disable CPCI backplane reset:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>Shell> kresetconfig pcislave off Reset from system master is disabled</pre>



6.2.12 kwdt uEFI Shell Command

kwdt

FUNCTION:	Configure the Kontron onboard Watchdog
SYNTAX:	<pre>kwdt [-? -t <timeindex>]</pre> <p>where:</p> <ul style="list-style-type: none"> -? Show help -t <timeindex> Configure the Watchdog with the time related to timeindex and activate it with reset routing <p>Call kwdt -h to obtain a list of time index values and related times</p>
DESCRIPTION:	The kwdt command allows to enable the Kontron onboard Watchdog with reset target before OS boot. This can be used to detect if the OS fails to boot and react by reset. The OS Watchdog driver is required for this functionality to operate.
USAGE:	<p>Get help:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>Shell> kwdt -?</pre> <pre>-t [time] - set Timer value 0 = 125ms value 1 = 250ms value 2 = 500ms value 3 = 1s value 4 = 2s value 5 = 4s value 6 = 8s value 7 = 16s value 8 = 32s value 9 = 64s value 10 = 128s value 11 = 256s value 12 = 512s value 13 = 1024s value 14 = 2048s value 15 = 4096s</pre>
USAGE:	<p>Set Watchdog to 16 seconds and activate it</p> <p>COMMAND / RESPONSE EXAMPLE (none):</p> <pre>Shell> kwdt -t 7</pre> <p>Note: Because there is no application which triggers the Watchdog, the system will be reset after 16 seconds in this case. This command should be invoked from a script, followed by an operating system boot, and the OS then has to start triggering the Watchdog.</p>
	<p>Display Watchdog configuration:</p> <p>COMMAND / RESPONSE EXAMPLE:</p> <pre>Shell> kwdt</pre> <pre>Kontron Board Watchdog Configuration: Watchdog Configuration Register (0x28C): 0x00</pre>



6.3 uEFI Shell Scripting

6.3.1 Startup Scripting

If the ESC key is not pressed and the timeout is run out, the uEFI Shell tries to execute some startup scripts automatically. It searches for scripts and executes them in the following order:

1. Kontron flash-stored startup script
2. If there is no Kontron flash-stored startup script present, the uEFI-specified `startup.nsh` script is used. This script must be located on any of the attached FAT formatted disk drives under `\efi\boot\startup.nsh`.
3. If none of the startup scripts is present or the startup script terminates, the default boot order is continued.

6.3.2 Create a Startup Script

Startup scripts can be created using the uEFI Shell built-in editor `edit` or under any OS with a plain text editor of your choice. To create a startup shell script, simply save the script on any FAT-formatted drive attached to the system under the file name `\efi\boot\startup.nsh`. To copy the startup script to the flash use the `kbootnsh` uEFI Shell command.

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the flash bank.

6.3.3 Examples of Startup Scripts

6.3.3.1 Automatic Booting from USB Flash Drive

Automatic booting is made from a USB flash drive, if present, otherwise the boot is made from the harddrive.

```
kboot -t usb-harddrive  
kboot -t harddrive
```

If neither a USB flash drive nor a harddrive is present, the boot order is continued.

6.3.3.2 Switch On Clock Spreading Prior to Booting from Harddrive

```
kclsp -e  
kboot -t harddrive
```

If no harddrive is present, the default order is continued.

6.3.3.3 Execute Shell Script on Other Harddrive

This example executes the shell script named `bootme.nsh` located in the root of the first detected disc drive (`fs0`).

```
fs0:  
bootme.nsh
```




6.3.3.4 Enable Watchdog and Control PXE Boot

The uEFI Shell provides environment variables used to control the execution flow.

The following sample start-up script shows two uEFI Shell environment variables, `wdt_enable` and `pxe_first`, used to control the boot process and the Watchdog.

```
echo -off
echo "Executing sample startup.nsh..."
if %wdt_enable% == "on" then
    kwdt -t 15
    echo "Watchdog enabled"
endif
if %pxe_first% == "on" then
    echo "forced booting from network"
    kboot -t network
endif
```

To create uEFI Shell environment variables, use the **set** uEFI Shell command as shown below:

```
Shell> set wdt_enable on
Shell> set pxe_first on
Shell> set
    pxe_first : on
    wdt_enable : on
Shell> reset
```



6.3.3.5 Handling the Startup Script in the Flash Bank

In case there is no mass storage device attached, the startup script can be generated in a RAM disk and stored in the flash bank using the following instructions:

4. Press <ESC> during power-up to log into the uEFI Shell.
5. Create a RAM disk and set the proper working directory as shown below:

```
Shell> kmkramdisk -s 3 myramdisk
Shell> myramdisk:
```

6. Enter the sample start-up script mentioned above in this section using the **edit** uEFI Shell command.

```
myramdisk:\> edit boot.nsh
```

7. Save the start-up script to the uEFI flash bank using the **kbootnsh** uEFI Shell command.

```
myramdisk:\> kbootnsh -p boot.nsh
```

8. Reset the board to execute the newly installed script using the **reset** uEFI Shell command.

```
myramdisk:\> reset
```

9. If a script is already installed, it can be edited using the following **kbootnsh** uEFI Shell commands.

```
myramdisk:\> kbootnsh -g boot.nsh
myramdisk:\> edit boot.nsh
```



Chapter

7

Updating the uEFI BIOS



This page has been intentionally left blank.





7. Updating the uEFI BIOS

BIOS updates are typically delivered as an update CD ISO image. This ISO image needs just to be burned to a CD and booted. Follow the menu for updating the uEFI BIOS. For further information refer to the update CD documentation.

7.1 uEFI BIOS Fail-Over Mechanism

The CP6004-SA/-RA/-RC/CP6004X-SA has two SPI boot flashes programmed with the uEFI BIOS, a standard SPI boot flash and a recovery SPI boot flash. The basic idea behind that is to always have at least one working uEFI BIOS flash available regardless if there have been any flashing errors or not.

7.2 Updating Procedure

An update CD is provided for flashing the latest uEFI BIOS on the standard SPI boot flash. The standard SPI boot flash can also be programmed with the latest uEFI BIOS via the **kflash -p** uEFI Shell command.

Note: To have the same content in both SPI boot flashes, clone the standard SPI boot flash to the recovery SPI boot flash. For further information, please refer to Chapter 6.2.7, kflash uEFI Shell Command.

Warning: Prior to updating or cloning the uEFI BIOS ensure that the ME FW Image Re-Flash function in the Main Setup menu is set to Enable (refer to Chapter 2.4.1 for further information). Failure to comply with the above may lead to a corrupt SPI boot flash content.

7.3 uEFI BIOS Recovery

In case of the standard SPI boot flash being corrupted and therefore the board not starting up, the IPMI controller boots the board from the recovery SPI boot flash if the DIP switch SW1 (CP6004-SA/CP6004X-SA) / SW3 (CP6003-RA), switch 2 is set to OFF. On the CP6004-RC, the configuration resistor R759 must be set to Open in order for the IPMI controller to boot the board from the recovery SPI boot flash.

For further information about the boot configuration, refer to the respective chapters in the board's user guide or contact Kontron for further assistance. Information about the boot configuration for the CP6004-SA/CP6004X-SA is provided in the CP6004-SA/CP6004X-SA User Guide, Chapter 4.1, for the CP6003-RA in the CP6004-RA/-RC User Guide, Chapter 4.1 and for the CP6004-RC in the CP6004-RA/-RC User Guide, Chapter 4.2.

7.4 Determining the Active Flash

Sometimes it may be necessary to check which flash is active. On the AMI Aptio-based uEFI BIOS, the information is available using the **kboardinfo** uEFI Shell command. For further information, refer to Chapter 6.2.2, kboardinfo uEFI Shell Command.



This page has been intentionally left blank.

