SourcePoint® For AMD 1.0 Release Notes

Copyright (c) 1994-2023 by ASSET InterTech, Inc.

Content

Contact Us

Phone	888-694-6250 (toll free) or +1-972-437-2800 (outside U.S.)
Contact Info	https://www.asset-intertech.com/support

Requirements

Host Operating Systems Supported
Windows 10, 11

Note: You may need to contact your systems administrator to gain administrator privileges on your host computer to properly install SourcePoint. The Installation wizard may give false errors of other uninstall programs running when administrator privileges are not enabled.

New Features and Bug Fixes

VERSION 1.0

Build 49 – January 11, 2023

Bergamo Support - Bergamo support has been added. Both single package and dual package have been validated.

Siena Support - Siena support has been added.

AP Wake Speedup - After a Go from reset, the target halts as each AP (application processor) wakes up. Previously, the user had to manually press Go to resume the boot process. SourcePoint now detects this condition, and automatically resumes execution.

The following Trouble Tickets (TT) have been resolved:

TT-16502: The second Go/Stop from the reset vector shows BADFOOD in the Registers window.

TT-16129: When hitting Go from the Reset vector, normal AMD platform behavior is to halt at each application processor (AP) wakeup. These extraneous halts slow down the boot process and make debugging more difficult. SourcePoint now automates this so the halt can be avoided.

TT-16589: Software breakpoint fix on Bergamo.

TT-16429: On Milan and Bergamo, the "Cause" command has been fixed, to rectify intermittent displays of "Unknown Reason" in the tooltips of the Viewpoint window's thread display when a breakpoint was hit.

TT-16591: Module flat32 within SecCore.pdb has multiple source files, and the source code was not being displayed within the SourcePoint Code window.

TT-16594: After setting a breakpoint from the Symbols window, the Breakpoints window shows an extraneous hyphen ("-") in the address string, i.e. main 00004004CCP-.

TT-16605: Breakpoints may fail or report incorrectly after unspecifying range breakpoints.

TT-16590: Cannot use a range breakpoint and a value breakpoint at the same time. The resolution is to add the second breakpoint, but it gets added as disabled, similar to what happens if you try to set breakpoints over the hardware breakpoint limit.

Build 45 – July 14, 2022

Genoa B0 Support – Genoa B0 parts have been validated with 4+1 and 12+1 silicon configurations. Both single package, and dual package have been validated.

Advanced Breakpoint Support – Three breakpoint enhancements have been added. All are additions to hardware breakpoints (those based on the debug registers):

1. Don't Cares are now allowed in breakpoint addresses. This allows breaking on a range with a single debug register. Supported on Milan, Genoa and later EPYC processors.
2. Up to two address ranges can be specified. Rather than breaking on a specific address, you can break when any address in a range occurs. This only applies to

data breakpoints. Range breaks consume two debug registers. Supported on Milan, Genoa and later EPYC processors.

3. A data value can be associated with a data access, so that a break only occurs when that value is read or written. Supported on Genoa and later EPYC processors.

Build 40

MCE Breakpoint Support – Machine Check Exception breakpoint support has been added.

UEFI gcc Support – Debug of UEFI code compiled with gcc is now supported.

Build 38

LBR Trace Support – Instruction trace utilizing the LBR MSRs has been added. This can be configured and viewed in the Trace View.

Genoa A0 Support – 12 CCD configuration has now been validated. Dual package support has also been validated.

Build 33

Genoa Support - Support for AMD Genoa A0 processors.

Build 32

PCI Devices View - Problem with missing entries has been fixed.

Build 30

Milan Support - Support for AMD Milan B0 processors. SMT silicon now tested. Secure Debug Unlock (SDU) now supported.

SDU Proxy Server Support - Secure Debug Unlock (SDU) now supports using a proxy server to access the AMD Key Distribution Server (KDS).

Down-binned cores - The Viewpoint view now correctly shows down-binned cores as "Not Active" rather than "running".

Build 25

Milan Support - Support for AMD Milan A0 processors. Includes 1P and 2P support. Only non-SMT silicon has been tested at this time.

Build 23

SDU Support - Support for Secure Debug Unlock (SDU). SourcePoint accesses the AMD Key Distribution Server (KDS) to get an unlock token for debugging secured silicon.

PEIM Debug - Fixed an issue with UEFI PEIM debug.

Build 20

Rome Support - Support for AMD Rome and Castle Peak processors. Includes 1P and 2P support.

Errata

VERSION 1.0

Build 49

Debugging from early SEC/PEI on secured parts requires the use of a JMP $ spinloop prior to initiation of the SDU session.

If a halt is performed directly in the middle of AP Wake code, AP's need to be individually woken up either with sequential Go/Stop or with a macro.

Bergamo and Siena appear as Genoa in the Viewpoint window.

Build 45

When breaking on a data value with mask and "Don't Cares" in the first two nibbles, prior to all APs being awake, SourcePoint will lose control and exhibit "BADFOOD" in the registers window. Example:

Connect to target with SourcePoint AMD 1.0.45
Turn on target and let it boot to EFI
Reset and wait
Step 2x
Set BP IO access Port 80 with DW data= B000A634
Hit Go
BP will hit. All threads enabled, and there is no issue here.

Reset and wait
Step 2x
Set BP IO access Port 80 with DW data= B000A63X
Hit Go

BP will hit. Only one thread enabled, and all Register values show 0BADFOOD
SourcePoint will have lost control of the target at this point.

Note that DW data = B000A634 works fine.
DW data = B000A6X4 or B000A6XX will also cause BADFOOD issue.

Build 33

Tested on AMD Onyx platform with 2+1 silicon. Dual package has not yet been validated. SDU has not yet been validated.

ZMM register display not yet supported.

Build 25 and earlier

Secure Debug Unlock (SDU) – The unlock process must be initiated at least 10 seconds after power-on or completion of reset.

Recommend procedure connection to a target with secured silicon from power off:

1. Power on the ECM-XDP3e.
2. Power on the target.
3. Wait approximately 10 seconds, then start SourcePoint. The target configuration macro will automatically run the unlock command. Enter your credentials in the dialog, and click OK.

When resetting or power-cycling the target while already connected, the same 10 second restriction after power-on or reset completion applies. In this case the unlock command is not automatically run, so open the Command window and enter "unlock" in the window to initiate the unlock process.

Viewpoint View Status – The viewpoint view shows missing or down-binned processors as "Not Active". The status of down-binned processors may show as "Stopped" during early boot code, following a reset or power cycle.

Project Reload Bug - When loading or reloading a project file, if prompted to select from the Project File or Emulator Configuration for the Device Configuration, select the Emulator Configuration. Selecting the Project File will cause a timeout in the communication with the emulator.

Reset and Power Cycle Support – In order to reset a Rome target the yellow and black twisted wire must be connected from the Reset pins on the ECM-XDP3e to the Rst Btn switch on the target. The Ethanol-X target has a two-pin header adjacent to the button on the board.

When resetting a Rome target the following events occur:

1. The debug tool commands reset to the target by shorting the yellow and black wires together. This simulates a button press.
2. The target begins the reset process.
3. The POST code LEDs on the board change to track progress before the processor de-asserts the reset signal to the debug tool.
4. It can take several seconds (more than 10 in some cases) for the target to reach IntChk1 and de-assert reset.
5. When the target stops after reset the IP register will show 0x1710 or similar address, the location of IntChk1. The code window disassembly may look strange.
6. Step the target to proceed to IntChk2. The Opcode at the instruction pointer is 0xFF. This is normal.
7. Step the target to proceed to the reset vector.

Power cycle break works similarly to Reset break, stopping after several seconds of POST codes at IntChk1.

Phantom Stops After Reset - When running an AMD target from the reset vector after a reset or power cycle, each AP thread may halt system execution as it is dispatched. Use the Go command (or the GUI equivalent) to continue execution. Loading the EFI.mac macro file will provide a user-defined macro button labeled "RunToAPWakeCompletion".

This macro is intended to run the target repeatedly until the last AP thread has been enabled. The underlying macro, EfiBtn10_Act.mac, uses “num_processors – 2” as the last processor number. This may not work in all CPU configurations and may need to be altered to “num_processors – 3” or similar, depending on how the down-binned processors are configured.

SMM Entry Breakpoint – The SMM Entry breakpoint relies on the SMM Base MSR for the address for setting the breakpoint. The SMM Base MSR has a reset value of 0x30000. The SMM Base MSR will get written with a new value at some point in the UEFI code, so an SMM Entry breakpoint will become ineffective when running from before the modification of the SMM Base MSR register by the code running on the target. The SMM Base MSR value is read for the SMM Entry breakpoint on each Go, so the SMM Entry breakpoint address is updated on every Go to reflect the current value of the SMM Base MSR.

ECM-XDP3e

The table below describes the behavior of the status LEDs on the front of the ECM-XDP3e:

STS	Lights briefly after emulator has performed boot-level hardware initialization and prior to loading flash image. Also, the upper and lower amber LEDs flash in an alternating patterr flash file fails to load.
RST	When lit, the target is in reset mode.
RUN	When lit, the target is running.
PWR	When lit, the emulator's power is on.

The table below describes the behavior of the network LEDs on the back of the ECM-XDP3e:

100MBT	When lit, the emulator is communicating at 100 Mb/s
1000MBT	When lit, the emulator is communicating at 1000 Mb/s

THIRD-PARTY COPYRIGHT NOTICES

OpenSSL

LICENSE ISSUES
==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/* ==
* Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.

*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ‘‘AS IS’’ AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
==========
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscape SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are adhered to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ''AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]