



Aptio AMISCE 5.03 User Guide

Aptio AMISCE version 5.03: User Guide

Document Revision 1.54

May 29, 2017



Confidential, NDA Required
Copyright ©2017

American Megatrends, Inc.
5555 Oakbrook Parkway
Suite 200
Norcross, GA 30093 (USA)

All Rights Reserved
Property of American Megatrends, Inc

Legal

Disclaimer

This publication contains proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, American Megatrends, Inc. American Megatrends, Inc. retains the right to update, change, modify this publication at any time, without notice.

For Additional Information

Call American Megatrends, Inc. at 1-800-828-9264 for additional information.

Limitations of Liability

In no event shall American Megatrends be held liable for any loss, expenses, or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential, arising from the design or use of this product or the support materials provided with the product.

Limited Warranty

No warranties are made, either expressed or implied, with regard to the contents of this work, its merchantability, or fitness for a particular use. American Megatrends assumes no responsibility for errors and omissions or for the uses made of the material contained herein or reader decisions based on such use.

Trademark and Copyright Acknowledgments

Copyright ©2017 American Megatrends, Inc. All Rights Reserved.

American Megatrends, Inc.
5555 Oakbrook Parkway
Suite 200
Norcross, GA 30093 (USA)

All product names used in this publication are for identification purposes only and are trademarks of their respective companies.

Table of Contents

Document Information	5
Purpose	5
Audience	5
Revision History	5
Overview	8
What is AMISCE?	8
AMISCE Features	8
System Requirements	9
Supported Operating Systems	9
Interface Descriptions.....	11
User Interface	11
Command Line Interface	11
Default Mode Execution	11
Default export mode	11
Handling Duplicate Questions	12
Handling suppressed and grayedout controls and forms	13
Raw mode execution	14
Raw export mode	14
Updating NVRAM with Script File.....	14
Default import mode	14
Disable Boot Option	15
BIOS without FixedBootOrder Module.....	15
BIOS with FixedBootOrder Module.....	16
Raw import mode	16
NVRAM Variable Access Unlock.....	17
Change User/Admin Password	17
Examples of password types used with password switches	18
PLDM Support	19
PLDM Export	19
PLDM Import	19
Single Question Update from Command Line	20
Examples for Single Question Update	20
Disable Boot Option.....	21
Read Single Question from Command Line.....	21
Example to read Single Question Value from Command Line	22
Sample Report	22
Default Output with Verbose option.....	22
Raw Mode Outputs.....	24
Variable Listing File	24
Instructions on using AMISCE.....	24
Default Mode Usage (/s).....	24
Raw Mode Usage (/n).....	26
Creating a New NVRAM Variable.....	28
SCE User Password.....	28

Setting Passwords	30
Passwords in Aptio	30
Steps to setup a Password	30
Example for changing Password without providing a Variable	30
Limitations.....	31
Appendix.....	32
BIOS Configuration Requirements	32
Error and Warning Messages	33
Linux/BSD Pre-Requisites (does not apply to ArmSceLnx)	34
REFERENCES	36
Signing Driver on RHEL 7 and Enrolling Public Key to the System	36
SCE Exit Codes	37

Document Information

Purpose

This document is intended to provide all the necessary information for using AMI Setup Control Environment (AMISCE) Tool.

Audience

The intended audiences are BIOS developers, Generic Chipset Porting Engineers, OEM Porting Engineers, and AMI OEM Customers.

Revision History

Date	Rev	Description of Changes
2009-09-09	0.10	Initial document created
2009-10-07	0.11	Document updated to provide windows OS support
2010-02-18	0.12	Document updated to include Windows 7 OS support
2010-03-05	0.13	Document updated with Advanced script File support
2010-04-07	0.14	Updated title page, header, document properties, features, and user interface.
2010-05-04	0.15	Add DOS SCE
2010-05-11	0.16	Added a note about '/f' option.
2010-06-08	0.17	Addressed Style Issues and updated content
2010-08-16	0.18	/u support clarified
2010-08-27	0.19	Removed /u option, clarified BIOS and Linux requirements
2010-09-02	0.20	Added exe name for all AMISCE version
2010-09-21	0.21	Updated the document with Password Encryption
2010-10-19	0.21	Fixed review comments
2010-10-26	0.21	Removed reference to UQI from AMISCE features
2010-12-22	0.21	Updated the document for Standards Review
2011-01-11	0.22	Added example for changing Password without providing a Variable
2011-01-12	0.23	Added description for manipulating NVRAM variables
2011-02-10	0.24	Add errors and warnings description to appendix
2011-03-14	0.25	Added note for basic intended use case
2011-04-06	1.01	Update for version 2.01
2011-07-21	1.02	Updated according to document standards.
2012-04-05	1.03	User password. BIOS requirements.
2012-07-30	1.04	APTIO V support
2012-10-04	1.05	Updated for release 2.02.1035ALPHA.
2012-12-17	1.06	Updated for adding /m support in SCEDOS.
2013-02-04	1.07	Add example of subtitle comment. Update and correct "Errors and Warnings". Change references to AFU to SCE in Linux driver section.
2013-03-25	1.08	Updated for adding /b support.

2013-06-07	1.09	Updated for adding /r support.
2013-06-15	1.10	Updated Question Evaluation support
2013-06-21	1.11	Updated for mapping language support
2013-07-18	1.12	Updated Instructions on using AMISCE
2013-08-05	1.13	Updated for /sp and /g support.
2013-10-11	1.14	Updated for 5.00.1048 release
2013-12-19	1.15	Updated With Creation of New NVRAM Variables
2014-01-02	1.16	Updated supported OS list
2014-01-16	1.17	Updated for provision to accept the mapping language.
2014-04-09	1.18	Updated the /a option in SCE to Enables Setup Question having Empty or Blank names to be exported in default export mode
2014-04-23	1.19	Updated for Option /d - Skip checking for AptioV BIOS and behave normally
2014-05-16	1.20	Added information regarding 'NVRAM Variable Access Unlock'
2014-06-25	1.21	Update system requirements. Explain "Platform Identification Failed" error message.
2014-07-24	1.22	Explain warning message for string controls
2014-07-28	1.23	Explain warning message for variable write
2014-09-24	1.24	Updated feature list with features for 5.01 and added information on new features. Added SCE Exit Codes section Updated BIOS requirements section
2014-10-14	1.25	Updated document header.
2014-10-14	1.26	Updated a note regarding exporting dynamic setup page questions.
2014-12-15	1.27	ARM CPU support
2015-01-29	1.28	Scan code and EFI key support
2015-02-04	1.29	Minor clarifications and additions
2015-05-04	1.30	SCE for ARM 64 EFI
2015-10-13	1.31	Added information on single question update from command line.
2015-10-22	1.32	Updated single question update usage with more options.
2015-10-30	1.33	Updated information on numeric value format for single question update from command line.
2015-11-05	1.34	Added information on mapping language for single question update.
2015-12-01	1.35	Revised Error and Warning Messages
2015-12-10	1.36	Updated for PLDM support
2015-12-21	1.37	Review update
2016-03-02	1.38	Updated copyright year
2016-03-03	1.39	Documentation standards update
2016-03-04	1.40	Fixed typos
2016-03-04	1.41	Added information to disable boot option
2016-03-04	1.42	Updated feature list
2016-03-17	1.43	Added BIOS requirements for disable boot option support.
2016-03-29	1.44	Added steps to sign driver on RHEL 7
2016-04-29	1.45	Updated information on disable boot option support when FixedBootOrder module present in BIOS.
2016-05-13	1.46	Updated for efivarstore variable type support
2016-06-21	1.47	Updated supported operating systems
2016-07-01	1.48	Updated FBO label information.
2016-07-05	1.49	Updated table of contents.
2016-08-16	1.50	Updated supported operating systems
2016-10-06	1.51	Updated information to read single question from command line,

		to identify grayedout and suppressed forms and controls in script, to hide banner, to specify multiple mapping languages and to use negative numbers as values for setup questions.
2016-10-21	1.52	Updated /sp and /g behavior for duplicate questions.
2017-01-16	1.53	Updated feature list.
2017-05-29	1.54	Updated information on handling duplicate questions.

Overview

What is AMISCE?

AMI Setup Control Environment (AMISCE) is a command line tool available in both 32-bit and 64-bit flavors. AMISCE provides you an easy way to update NVRAM variables from within the EFI, DOS, Linux, or Windows based environment. The user can extract variables directly from the BIOS, and also allows the user to change settings using either a text editor or a setup program, and then update the BIOS. Each of these actions may take place on a different system.

AMISCE produces a script file that lists all setup questions on the system where AMISCE is running. The user can then modify the script file and use it as input to change the current NVRAM setup variables.

AMISCE Features

The AMISCE tool allows you to perform the following functions:

1. Reads NVRAM variables and HII database from BIOS at run time to create files that can be used as input to a setup emulation program. The NVRAM script file may be edited as text.
2. Loads the NVRAM script file created by above process, and updates the target system's NVRAM.
3. Enables advanced scripting mode that presents data as setup questions and associated settings.
4. Enables advanced scripting mode to update setup question defaults.
5. Supports setup question matching based on Setup Mapping Language. This support will be available once Aptio core supports Setup Mapping Languages.
6. Provides Command line operation.
7. Supports APTIO V features.
8. Supports Setup Question Evaluation for UEFI 2.1 and above
9. Supports blocking of migration.
10. Supports to specify multiple mapping language.

11. Support to export only questions whose value is different from default.
12. Supports suppression of duplicate questions.
13. Unlocks protected variable update with administrator password.
14. Support to change user/admin password
15. Aptio V BIOS Identification.
16. Get SMI port from ACPI table
17. Support to allow raw import to change size of variable data
18. Supports managing duplicate/unmatched setup questions.
19. Support to export all questions and filter out questions with improper strings (also if no x-AMI entry).
20. Support to comment out duplication questions
21. Support for special controls and to implement string controls.
22. Supports Migration of Settings.
23. Boot order synchronization
24. Verbose mode for detailed generation of the script file.
25. Support for output subtitles as comments to SCE scripts
26. Support to show warnings when multiple questions share the same storage location
27. OFBD module password check support.
28. UEFI spec support
29. Build using Aptio V build environment in VeB
30. Support for UEFI Shell 1.x and 2.x.
31. ARM Support
32. Change question value from command line.
33. PLDM Support.
34. Support for efivarstore type variable.
35. Support for negative numbers as values for numeric controls.
36. Support to hide banner.
37. Support to read single question value from command line.
38. Support to identify suppressed and grayedout forms and controls in script file.
39. SMM communication support.

System Requirements

Supported Operating Systems

AMISCE is supported by the following operating systems:

- EFI Shell Environment
- Microsoft® DOS
- Microsoft Windows® 2000
- Microsoft Windows® NT 4.0
- Microsoft Windows® XP
- Microsoft Windows® ME
- Microsoft Windows® 2003
- Microsoft Windows® Vista
- Microsoft Windows® 7
- Microsoft Windows® 8
- Microsoft® Windows® 8.1
- Microsoft® Windows® Server 2008 R2
- Microsoft® Windows® Server 2012 R2
- Linux
- BSD
- Microsoft Windows® 10
- Windows PE
- Microsoft Windows Server 2016



Note: Starting From Microsoft Windows® 7 in all the windows Operating System the Application requires Administrator privileges to be executed and the command box is opened with *Run as Administrator* option.



Note: For accessing Linux and BSD versions refer the steps outlined in [Appendix](#) section.

Interface Descriptions

User Interface

The user has to execute the following command lines in command prompt to run AMISCE.

Command Line Interface



Note: In the examples given below, “AMISCE” should be replaced with the correct OS specific version name from the following list:

- For DOS use SCEDOS
- For WIN 32 utilize SCEWIN
- For WIN 64 utilize SCEWIN_64
- For LINUX 32 utilize SCELNX_32
- For LINUX 64 utilize SCELNX_64
- For LINUX ARM 64 utilize SceLnxArm
- For BSD 32 utilize SCEBSD_32
- For BSD 64 utilize SCEBSD_64
- For EFI 32 utilize SCEEFI.EFI
- For EFI 64 utilize SCEEFI64.EFI
- For EFI ARM 64 utilize SceEfiArm

Default Mode Execution

The default mode of execution provides the ability to export and import NVRAM setting values for BIOS setup controls using a script. It can optionally generate the HII dump file.

Default export mode

To enable the default mode execution execute the command line

```
AMISCE /o /s <Setup Script File> [/h <HII Dump File>] [/sd  
<Duplicate Question Script File>] [/b] [/v] [/lang <Lang  
Code1,Langcode2,LangcodeN>] [/sp] [/g] [/a] [/d] [/q] [/ndef]  
[/ce] [/hb]
```

Where,

/o → Indicates generate Setup script file form HII data

/s → Indicates Setup script file that is to be generated.

[/h]→Indicates the HII Dump File, it is an optional feature, where this valid only while generating Setup script file

[/v]→Optional CMD line that produces a verbose script file

[/b]→ Optional CMD line option that enables export of boot order controls in the generated script file.

[/lang]→ Optional CMD line option that enables mapping language mode which will export questions with the specified lang codes. Lang Code indicates the code for a particular languages like for English(en-US), AMI(x-AMI) etc.

[/sp] → Optional CMD line option that enables Expression Evaluation for Suppressif Opcode.

[/g] → Optional CMD line option that enables Expression Evaluation for Grayoutif Opcode.

[/a] → Optional command line option that enables setup question having empty or blank names to be exported

[/d] → Optional command line option to Skip checking for AptioV BIOS and behave normally

[/ndef] → Optional command line option to export only those questions whose value is different from the default.

[/sd] → Optional command line option to export duplicate questions in to a separate script file.

[/ce] → Optional command line option to specify with /sp and/or /g which comment out suppressif and grayoutif setup questions and forms.

[/hb] → Optional command line option to hide the tool information banner.

The user may optionally give the **/q** option to suppress all warning messages.



Note: The user has to use **SCEWIN** as windows executable command, but while using DOS the executable command will be **SCEDOS**. Numeric questions with decimal value(including negative values) will be mentioned inside angular brackets.

Handling Duplicate Questions

SCE considers questions with same storage location as duplicates. By default, these duplicates will be exported to the main script file but will be commented out. To export the duplicates into a separate script file, use the '**/sd**' option.

SCE won't import commented out questions, It will treat commented out questions as it doesn't exist in script. To import a commented out question, user have to remove the comment out symbols **"//"** and then import as shown below.

Example of commented out question,

```
// Setup Question      = S/W Error Injection Support
// Token              =400    // Do NOT change this line
// Offset=90
// Width =01
// BIOS Default =[00]Disable
// MFG Default =[00]Disable
// Options          =*[00]Disable    // Move "*" to the desired Option
//                [01]Enable
```

To import the commented out question, Change it as shown below and then import.

```
Setup Question = S/W Error Injection Support
Token  =400    // Do NOT change this line
```

```
Offset =90
Width =01
BIOS Default =[00]Disable
MFG Default =[00]Disable
Options =[00]Disable // Move "*" to the desired Option
           [01]Enable
```



Note: Questions in dynamic pages will not be available in exported script until these pages are visited in setup. Questions which are inside suppressif or grayoutif conditions only will be removed from script for /sp or /g command respectively, Duplicate instances of the same questions which are not inside suppressif or grayoutif conditions will not be removed.

Handling suppressed and grayedout controls and forms

SCE indicates forms and setup questions present inside suppressif and grayoutif conditions. These questions will be exported to the main script in commented form when '/ce' option is mentioned with /sp and/or /g option. An illustration of forms and controls inside grayoutif and suppressif conditions is shown below.

```
// SUPPRESS FORM

// SUPPRESS
// Setup Question = Test1
// Token =40 // Do NOT change this line
// Offset =02
// Width =01
// BIOS Default =[01]Enabled
// Options =[00]Disabled // Move "*" to the desired Option
//      *[01]Enabled
// ENDOF SUPPRESS

// Setup Question = Test2
// Token =51 // Do NOT change this line
// Offset =22
// Width =01
// BIOS Default =[01]Enabled
// Options =[00]Disabled // Move "*" to the desired Option
//      *[01]Enabled

// GRAYOUT
// Setup Question = Test3
// Token =271B // Do NOT change this line
// Offset =48B
// Width =01
// BIOS Default =14
// Value =21
// ENDOF GRAYOUT

// ENDOF SUPPRESSED FORM

// GRAYOUT FORM

// Setup Question = Test4
// Token =33F // Do NOT change this line
// Offset =F3E
// Width =01
```

```
// BIOS Default  =[00]None
// Options       =[00]None    // Move "*" to the desired Option
//      [01]Option1
//      [02]Option2

// END OF GRAYED OUT FORM
```

As shown above, if a form is present under grayoutif or suppressif, the controls present in that form will be shown in commented form.

Raw mode execution

AMISCE raw mode execution can export and import all NVRAM variables, including those not used for setup purposes. It also generates the listing file and HII dump file.

Raw export mode

```
AMISCE /o [/c] /l <listing file> /n <NVRAM Dump File> /h <HII
dump file> [/d] [/hb]
```

Where,

/o→ Indicates NVRAM script file to generate for Variables found in Listing File

/l→ Indicates Variable Listing File

/c→ Optional, Creates Variable Listing File containing information about all the variables found in NVRAM

Where,

With /c option, all variables names are output to the listing file, and all variables are output to the NVRAM dump script.

Without /c option, the listing file serves as a filter and the program provides output only to those variables with names present in the listing file.

/n→ Indicates NVRAM Dump File

/h→ Indicates HII Dump File. This option is valid only when generating NVRAM script file and should always be used along with the /n option.

/d]→ Optional command line option to Skip checking for AptioV BIOS and behave normally

/hb→ Optional command line option to hide the tool information banner.

Updating NVRAM with Script File

Updating the NVRAM variables associated with setup questions can be achieved using the following commands.

Default import mode

```
AMISCE /i [/cpwd | /cpwds | /cpwde <admin password>] /s <Setup
Script File> [/ds] [/dm] [/b] [/r] [/lang <Lang Code 1,Lang
Code 2,Lang code N>] [/d] [/hb]
```

Where,

[/cpwd] → Indicates admin password of type unicode
[/cpwds] → Indicates admin password of type scan code
[/cpwde] → Indicates admin password of type EFI key
/i → Indicates Import modified script file to the NVRAM
/s → indicates the NVRAM script file to use to read data
/ds → Indicates set "BIOS" defaults from script question value
/dm → Indicates set "MFG" defaults from script question value
[/b] → Optional CMD line option that enables import of boot order controls from the generated script file.
[/r] → Optional CMD line option in SCEWIN, SCEEFI, SCEBSD, SCELNX that enables the tool to verify that the CRC32 of host HII IFR packs is identical to the CRC32 in the advanced script file before performing any variable updates. If not identical, then the application exits with relevant error message.
[/lang] → Optional CMD line option that enables mapping language mode which will import questions with the specified lang codes. Lang Code indicates the code for a particular languages like for English(en-US), AMI(x-AMI) etc.
[/d] → Optional command line option to Skip checking for AptioV BIOS and behave normally
[/cpwd | /cpwds | /cpwde] → Unlock variables with administrator password until AMISCE completes execution.
[/hb] → Optional command line option to hide the tool information banner.

The user may optionally give the **/q** option to suppress all warning messages.

Disable Boot Option

SCE supports disabling boot options in default import mode.

BIOS without FixedBootOrder Module

When FixedBootOrder module is not present, SCE supports disabling only legacy boot options. To disable a legacy boot option, follow below steps:

1. Export the script in advanced mode with **/b** option.
2. Change the higher order byte of the boot option to be disabled to 'FF'.
3. Import the script with **/b** option.

For example, consider the below legacy device boot order:

```
Setup Question      = BBS_TYPE_HARDDRIVE Boot Option #
Map String          = SETUP006
Token               = 9F0 // Do NOT change this line
Offset=00
Width=02
ListOrder           = [0019]BBS_TYPE_HARDDRIVE 0019
                    [001b]BBS_TYPE_HARDDRIVE 001b
```

To disable the first boot option, change the entry as below and import the script with **/b** option.

```
Setup Question      = BBS_TYPE_HARDDRIVE Boot Option #
Map String          = SETUP006
Token               = 9F0 // Do NOT change this line
Offset=00
Width=02
```

```
ListOrder      = [FF19]BBS_TYPE_HARDDRIVE 0019  
                [001b]BBS_TYPE_HARDDRIVE 001b
```

BIOS with FixedBootOrder Module

When FixedBootOrder module is present, SCE supports disabling both legacy and UEFI boot options. To disable a boot option, follow below steps:

1. Export the script in advanced mode with /b option.
2. Choose 'Disable' for the boot option to be disabled.
3. Import the script with /b option.

For example, consider the below boot option:

```
Setup Question = Boot Option #2  
Map String     = Boot Option #2  
Token         =1345 // Do NOT change this line  
Offset        =145  
Width         =01  
BIOS Default   =[01]Windows Boot Manager (P3: ST500DM002-1ER14C)  
Options        =[00]ubuntu (P1: ST500DM002-1BC142) // Move "*" to the desired Option  
               * [01]Windows Boot Manager (P3: ST500DM002-1ER14C)  
               [12]Disable
```

To disable, move '*' to 'Disable' entry and import the script with /b option.

```
Setup Question      = Boot Option #2  
Map String          = Boot Option #2  
Token               =1345 // Do NOT change this line  
Offset=145  
Width=01  
BIOS Default        =[01]Windows Boot Manager (P3: ST500DM002-1ER14C)  
Options              =[00]ubuntu (P1: ST500DM002-1BC142) // Move "*" to the  
desired Option  
                   [01]Windows Boot Manager (P3: ST500DM002-1ER14C)  
                   * [12]Disable
```

Raw import mode

```
AMISCE /i [/cpwd | /cpwds | /cpwde <admin password>] /l  
<listing file> /n <NVRAM Dump File> [/f] [/d] [/hb]
```

Where,

/cpwd→ Indicates admin password of type unicode

/cpwds→ Indicates admin password of type scan code

/cpwde→ Indicates admin password of type EFI key

/i→ Indicates Import modified Variable data found in Listing File to the NVRAM

/l→ Indicates Variable Listing File

/n→Indicates NVRAM Dump File

/d→ Optional command line option to Skip checking for AptioV BIOS and behave normally

/cpwd | /cpwds | /cpwde→ Unlock variables with administrator password until AMISCE completes execution.

/hb→ Optional command line option to hide the tool information banner.

The tool verifies that the CRC32 of host HII IFR packs is identical to the CRC32 in the variable file before performing any variable updates. Usage of the 'f' option will suppress this check.

NVRAM Variable Access Unlock

Runtime access to writing certain NVRAM variables may be locked out in some BIOS configurations. SCE can unlock them with the BIOS administrator password.

```
AMISCE [/cpwd | /cpwds | /cpwde] <administrator password>  
<other parameters>
```

Where,

[/cpwd]→ Indicates admin password of type unicode

[/cpwds]→ Indicates admin password of type scan code

[/cpwde]→ Indicates admin password of type EFI key

The variable access is re-locked on application exit. So, it is required to use /cpwd or /cpwds or /cpwde each time with import command for protected variable update. SCE shows the message "*Variable access re-locked*" on successful re-lock of the protected variables. It is important to re-lock the variables after update. User can explicitly do this by executing the import command with an incorrect admin password.

Also, there is a retry limit of 3 for the unlock attempt. If the retry limit is exceeded, then system reboot is required to try again.

Note: '/cpwd or /cpwds or /cpwde' cannot be used as stand-alone option.

Change User/Admin Password

SCE supports changing user/admin passwords for BIOS setup. The current admin password needs to be provided using /cpwd or /cpwds or /cpwde.

```
AMISCE [/cpwd | /cpwds /cpwde] <current admin password> [/apwd  
| /apwds | /apwde] <new admin password> [/upwd | /upwds /  
upwde] <new user password> [/hb]
```

Where,

[/cpwd]→ Indicates admin password of type unicode

[/cpwds]→ Indicates admin password of type scan code

[/cpwde]→ Indicates admin password of type EFI key

[/apwd]→ Indicates new admin password of type unicode

[/apwds]→ Indicates new admin password of type scan code

[/apwde]→ Indicates new admin password of type EFI key

[/upwd]→ Indicates new user password of type unicode

[/upwds]→ Indicates new user password of type scan code

[/upwde]→ Indicates new user password of type EFI key

[/hb]→ Optional command line option to hide the tool information banner.

Examples of password types used with password switches

Unicode Password usage:

AMISCE /cpwd test123 /apwd 123test /upwd test

Scan code Password usage:

AMISCE /cpwds 0x14 0x12 0x1F 0x14 0x02 0x03 0x04 /apwds 0x02 0x03 0x04 0x14 0x12 0x1F 0x14 /upwds 0x14 0x12 0x1F 0x14

EFI key password Usage:

AMISCE /cpwde 0x35 0x33 0x21 0x35 0x45 0x46 0x47 /apwde 0x45 0x46 0x47 0x35 0x33 0x21 0x35 /upwde 0x35 0x33 0x21 0x35

Note: 0x prefix is optional with Scan code and EFI key. Scan codes and EFI key codes mentioned above are according to keyboard layout English(United States)-US

PLDM Support

SCE supports exporting the setup configuration to PLDM data structures. This is useful especially while migrating the BIOS configuration. SCE generates a single binary file as output with all the PLDM data structures combined together. The exported PLDM file can then be imported using SCE to apply the configuration on the target system. The below commands can be used for export and import:

PLDM Export

```
AMISCE /o /p <PLDM file name> [/lang <Lang Code 1,Lang Code 2,Lang code N>] [/sp] [/g] [/b] [/ndef] [/hb]
```

Where,

/o → Export configuration command.

/p → Indicates PLDM file

/sp → Optional CMD line option that enables Expression Evaluation for Suppressif Opcode.

/g → Optional CMD line option that enables Expression Evaluation for Grayoutif Opcode.

/b → Optional CMD line option that enables export of boot order controls in the generated PLDM file.

/ndef → Optional command line option to export only those questions whose value is different from the default.

/lang → Optional CMD line option that enables mapping language mode which will export questions with the specified lang codes. Lang Code indicates the code for a particular languages like for English(en-US), AMI(x-AMI) etc.

/hb → Optional command line option to hide the tool information banner.

PLDM Import

```
AMISCE /i /p <PLDM file name> [/lang <Lang Code 1,Lang Code 2,Lang code N>] [/b] [/hb]
```

Where,

/i → Import configuration command.

/p → Indicates PLDM file

/b → Optional CMD line option that enables import of boot order controls from the input PLDM file.

/lang → Optional CMD line option that enables mapping language mode which will import questions with the specified lang codes. Lang Code indicates the code for a particular languages like for English(en-US), AMI(x-AMI) etc.

/hb → Optional command line option to hide the tool information banner.

Single Question Update from Command Line

This feature allows to update single setup questions from command line without using the script file. It makes use of the mapping language string to uniquely identify the question. The map string for a question can be known by exporting the script with '/lang' option. The '/lang' option will add the 'Map String' field for each setup question in the script. To use the '/lang' option, the Aptio firmware should have the mapping language enabled. The command line usage is shown below:

```
AMISCE /i [/cpwd | /cpwds | /cpwde <admin password>] [/lang  
<Lang Code 1,Lang Code 2,Lang code N>] /ms <map string> /qv  
<question value> [/bt <device type>] [/q] [/d] [/dm] [/ds]  
[/hb]
```

Where,

/i → Indicates Import question values to the NVRAM

/cpwd | /cpwds | /cpwde → Used to specify the current admin password. This option needed only if the variable to update is protected.

/lang → Optional command line to specify the mapping languages to look the setup question mapping string. The default is x-AMI and x-UEFI-AMI.

/ms → Used to specify map string for the particular setup question.

/qv → Used to specify the value for the setup question.

/bt → Used to mention the device type for legacy boot order update.

/q → Optional command line option to suppress all warning messages.

/d → Optional command line option to Skip checking for AptioV BIOS and behave normally

/ds → Optional command line option Indicates set "BIOS" defaults from question value.

/dm → Optional command line option Indicates set "MFG" defaults from question value.

/hb → Optional command line option to hide the tool information banner.

Examples for Single Question Update

Boot Order question:

The question value should be a comma separated list of boot devices where each boot device is represented using the unique number assigned to it in the UEFI boot order. The list should contain all devices in the current boot order.

AMISCE /i /ms SETUP001 /qv 0x0002,0x0001

Legacy Device Order question:

The question value should be a comma separated list of boot devices where each boot device is represented by the predefined token value associated with it. The list should contain all devices of the specified type in the current boot order. The boot device type string should be one of the below:

BBS_TYPE_FLOPPY
BBS_TYPE_HARDDRIVE
BBS_TYPE_CDROM
BBS_TYPE_PCMCIA
BBS_TYPE_USB

BBS_TYPE_EMBEDDED_NETWORK
BBS_TYPE_BEV
BBS_TYPE_UNKNOWN

The device type string is same as the first part of the legacy boot order Setup Question name in script.

AMISCE /i /ms SETUP002 /bt BBS_TYPE_HARDDDRIVE /qv 0x0019,0x001A

Language/Platform Language question:

The question value represents the index of the language in the list of supported languages.

AMISCE /i /ms SETUP003 /qv "<-10>"

Numeric question:

The question value represents the new value. This should be within the valid range.

AMISCE /i /ms SETUP004 /qv 0x09

Checkbox question:

The question value should be either 0 or 1.

AMISCE /i /ms SETUP005 /qv 0x01

One-of question:

The question value represents the index of the option in the list of options.

AMISCE /i /ms SETUP006 /qv 0x02

Note: String type questions are not supported currently. Decimal numeric value(including negative numbers) has to be mentioned with angular brackets (<>) and mentioning the angular brackets without quotation might lead to file redirection warnings. Numeric value will be taken as hexadecimal value (0x prefix is optional) if not mentioned in decimal format.

Disable Boot Option

SCE supports disabling legacy boot options from command line. To disable a boot option, specify the higher order byte of the entry to be disabled as 'FF'. An example is shown below:

> AMISCE /i /ms SETUP007 /bt BBS_TYPE_HARDDDRIVE /qv 0xff19,0x001a

Note: The BIOS should not have FixedBootOrder module. If FixedBootOrder module is present, use default import mode to disable boot options.

Read Single Question from Command Line

This feature allows to read single setup question's value from command line without using the script file. It makes use of the mapping language string to uniquely identify the question. The map string for a question can be known by exporting the script with '/lang' option. The '/lang' option will add the 'Map String' field for each setup question in the script. To use the '/lang'

option, the Aptio firmware should have the mapping language enabled. The command line usage is shown below:

```
AMISCE /o [/lang <Lang Code 1,Lang Code 2,Lang code N>] /ms  
<map string> [/q] [/hb]
```

Where,

/o→ Indicates export question values

/lang → Optional command line to specify the mapping languages to look the setup question mapping string. The default is x-AMI and x-UEFI-AMI.

/ms → Used to specify map string for the particular setup question.

/q → Optional command line option to suppress all warning messages.

/hb→ Optional command line option to hide the tool information banner

Example to read Single Question Value from Command Line

Command should contain the unique mapping string of the setup question as shown below.

```
AMISCE /o /ms setup00 /lang x-AMI
```

Sample Report

The following program sample illustrates the listing of file content, where the two NVRAM variables shown below contain their Name and GUID. All numeric values are in hexadecimal notation only.

Default Output with Verbose option

```
// Script File Name: script.txt  
// Created on 03/15/11 at 04:20:47  
// Copyright (c) 2011 American Megatrends, Inc.  
// AMISCE Utility. Ver. 5.02.1074  
  
HIICrc32 = 5CFC3E93  
  
// FORM SET  
// GUID      = ec87d643-eba4-4bb5-a1e5-3f3e36b20da9  
// Title     = Main  
// Help      = System Overview  
// Class     = 01  
// SubClass  = 00  
  
// FORM  
// FORM ID   = 01  
// Title     = Main  
  
Setup Question   = System Language  
Token =00      // Do NOT change this line  
Offset          =00  
Width =02  
BIOS Default     = [0] N/A  
MFG Default     = [0] N/A
```

```
Options      = *[00] English

// FORM SET
// GUID      = ec87d643-eba4-4bb5-a1e5-3f3e36b20da9
// Title     = Advanced
// Help      = Advanced Settings
// Class     = 02
// SubClass  = 00

// FORM
// FORM ID   = 02
// Title     = Advanced

Setup Question = Launch PXE OpROM
Token =00     // Do NOT change this line
Offset       =1B
Width =01
BIOS Default      = 00
MFG Default = 01
Value =1

// Subtitle = PCI Common Settings

Setup Question = PCI Latency Timer
Token =00     // Do NOT change this line
Offset       =03
Width =01
BIOS Default      = [20]32 PCI Bus Clocks
MFG Default = [20]32 PCI Bus Clocks
Options          =*[20]32 PCI Bus Clocks // Move "*" to the desired Option
                [40]64 PCI Bus Clocks
                [60]96 PCI Bus Clocks
                [80]128 PCI Bus Clocks
                [A0]160 PCI Bus Clocks
                [C0]192 PCI Bus Clocks
                [E0]224 PCI Bus Clocks
                [F8]248 PCI Bus Clocks

Setup Question = Setup Prompt Timeout
Token =00     // Do NOT change this line
Offset       =00
Width =02
BIOS Default      = 01
MFG Default = 01
Value =05
Setup Question = Boot Option #
Token =00     // Do NOT change this line
Offset       =00
Width =02
BIOS Default      = [0] N/A
MFG Default = [0] N/A
ListOrder = [0001] Built-in EFI Shell
            [0000] Hard Drive
            [0003] UEFI: PNY USB 2.0 FD PMAP
```

[0002] CD/DVD Drive

Raw Mode Outputs

Variable Listing File

```
[VARIABLE]
VARIABLE_NAME = MonotonicCounter
VARIABLE_GUID = 8be4df61-93ca-11d2-aa0d-00e098032b8c

[VARIABLE]
VARIABLE_NAME = SetupCpuFeatures
VARIABLE_GUID = ec87d643-eba4-4bb5-a1e5-3f3e36b20da9
```

The following sample illustrates the script file content, where the two types of NVRAM variables shown below contain their GUID, Attribute, Name and the data.

```
Version
00000001
HiiCrc32
2b147ed6

GUID
8be4df61-93ca-11d2-aa-0d-00-e0-98-03-2b-8c
Attributes
00000007
VariableName
MonotonicCounter
VariableData
06 00 00 00

GUID
61dfe48b-ca93-d211-aa-0d-00-e0-98-03-2b-8c
Attributes
00000007
VariableName
SetupCpuFeatures
VariableData
00 00 01 00 01 00 01 01 00
```

Instructions on using AMISCE

Default Mode Usage (/s)

- From CMD line environment execute AMISCE using the following command to generate the NVRAM script file:

```
'AMISCE /o /s <NVRAM.txt> [/h <Hii.db>] [/b] [/v] [/lang <en-US>]
[/sp] [/g]'
```

Where,

NVRAM.txt – NVRAM script file

hii.db – HII dump output file
en-US – Language code for English.

- Now open the generated script file and modify the required setup question value and save the modifications. You should remove any setup questions that you do not wish to update.
- Now from CMD line environment execute the following command:

```
AMISCE /i /s <NVRAM.txt> [/r] [/b] [/lang <en-US>]
```

Where,

NVRAM.txt – NVRAM script file
en-US – Language code for English.

- The new settings are updated into the NVRAM.
- The default export behavior without /b option will be not to export boot order controls. To enable exporting of boot order controls provide /b option.
- The default import behavior without /r option will not check whether CRC32 of host HII IFR packs is identical to the CRC32 in the advanced script file. To enable the verification of CRC32 value provide /r option.
- AMISCE will evaluate individual setup question expression, it will export the setup question into script file depends on the result, If the result obtained is suppress then that setup question will not be exported to the script file. Currently AMISCE supporting Suppress if alone. All the other conditions will not be evaluated by AMISCE.

Note: In order to evaluate the expression properly, the dependent NVRAM variable of the setup question should have runtime access.

Output script file will not have the suppressed setup questions.

- If /sp command is given while export operation and if expression evaluation results in suppress then AMISCE will not export the setup question to the script file. If /g command is given while export operation and if expression evaluation results in grayout, then AMISCE will not export the setup question to the script file.
- If /ce command is mentioned with /sp or /g then it will export the suppressed or grayed out controls and forms in commented format to the script file.
- AMISCE will export setup questions with mapstring if /lang option is provided. While importing if /lang option is there, it will check for setup question prompt and mapstring alone between advanced script file and host system.

For example, if in the script file a setup question is like :

```
Setup Question      = Setup Prompt Timeout  
Mapstring = BOOT001
```

```
Token    =00    // Do NOT change this line
Offset   =00
Width    =02
BIOS Default  = 01
MFG Default  = 01
Value    =05
```

And the command is given as : SCEWIn.exe /i /s Script.txt /lang , this will check for “Mapstring”. If it is not found the application will report an error.

- By default the mapping language is x-AMI and x-UEFI-AMI so if user gives /lang option alone then it will export setup questions with mapstring and output should contain both English and x-AMI strings. If user provides /lang option with a language code then SCE will check whether that language code strings are there in target machine if it is there it will export setup questions with mapstring and output should contain both English and that language code strings and if not, then will show a warning message and will export setup questions with mapstring value as “NULL”.
- While importing if /lang option is there the question matching should be done using the default mapping language string instead of the English string and if user gives /lang option with a language code then question matching should be done using that language code strings.

Note: Some BIOS contain duplicate setup questions. Before importing the script, any duplicate questions should be removed.

Raw Mode Usage (/n)

- AMISCE requires the knowledge of setup question offset to manipulate NVRAM variables. From windows environment execute AMISDE on the target firmware image using the command

```
'AMISDE /i <firmware image> /o <output report> /v'
```

For example,

While manipulating “Pxe Boot Option” setup question, the user can manually select the mode as either Enabled or Disabled by altering the predefined Width (0x0001) in the specified OFFSET value (0x000D) located in the output extracted using AMISDE.

For Disabled Mode,

```
Variable Name
Setup
Variable Data
00 01 20 00 00 00 00 00 01 37 37 37 00 00 02 00
00 FF 00 00 00 00 00 00 00 37 00 00 00 00 00 00
02 00 01 00 01 00 00 00 00 00 00 00 00 00 00 01
00 03 03 01 FF 01 01 00 08 00 00 00 00 01 00 00
01 01 01 01 FE 00
```

For Enabled Mode,

```
Variable Name
Setup
Variable Data
00 01 20 00 00 00 00 00 01 37 37 37 00 01 02 00
00 FF 00 00 00 00 00 00 00 37 00 00 00 00 00 00
02 00 01 00 01 00 00 00 00 00 00 00 00 00 00 01
00 03 03 01 FF 01 01 00 08 00 00 00 00 01 00 00
01 01 01 01 FE 00
```

- Open the report file and browse for the setup question values that need to be changed. Note down the Variable Name and Variable GUID for the setup questions that need the values changed.
- Now create a Variable Listing file for input to AMISCE with the Variable information collected previously. **Many variables are used for purposes other than setup question data so you should take care to update only the desired variable.** The listing file format is as described above.
- Now from the CMD line environment execute AMISCE using the following command to generate the NVRAM script file:

```
'AMISCE /o /h <Hii.db> /l <Listing.txt> /n <NVRAM.txt>'
```

Where,

Listing.txt - Variable listing file created in the previous step.

Hii.db - HII dump output file

NVRAM.txt - NVRAM variable script output file in ASCII format

- Now open AMISDE report file to get a setup question's offset and width.
- Open the NVRAM script file for modification.
- Get the question's offset and data width, to modify a setup question's value. In the NVRAM script file, locate the correct Variable data, and change the data values. The Variable Data are formatted with 16-bytes in a line with each byte separated by a space.
- Once all the modification to the NVRAM file is done from the CMD line environment, execute the following command to save the values back into NVRAM

```
'AMISCE /i /l Listing.txt /n NVRAM.txt'
```

Where,

Listing.txt - Variable Listing file

NVRAM.txt - NVRAM variable script file is modified in previous step.

- The new settings are now updated into the NVRAM.



Note: AMISCE provides a complete listing of all the questions or variables available in the BIOS, and the user can alter/remove any setting in the script according to their needs. Once the script is modified, they can use their modified script for the installation of these new settings. When

importing settings to a different machine you should take care to remove questions that may have values not appropriate for the new environment.

Creating a New NVRAM Variable

Using Raw Mode Export Command generate the list file and nvram script file.

AMISCE /o /c /l list.txt /n nvram.txt /h Hii.db

Now Open the list.txt and add the new variable to listing file like

New Variable

```
[VARIABLE]
VARIABLE_NAME = XYZ
VARIABLE_GUID = xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

And Open nvram.txt file and Add new variable, Attributes and Variable Data

New Variable

```
GUID
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Attributes
xxxxxxx
Variable Name
XYZ
Variable Data
xx xx xx xx xx xx .. .. .
```

Then using import command Import the script file To Update New Variable in NVRAM

AMISCE /i /l List.txt /n nvram.txt

To check whether the new variable is created or not. Then generate list and nvram file again using export command

AMISCE /o /c /l list_new.txt /n nvram_new.txt /h Hii_new.db

Open and check the new variable is present or not in list_new.txt as well as in nvram_new.txt file check variable specified above.

SCE User Password

The BIOS may be optional configured to request a password from the SCE user. The user will receive a password prompt when performing import operations. If the user fails to enter the correct password within the maximum value for the password entry counter configured in the BIOS, he will have to reset the computer to clear the counter.



Setting Passwords

Passwords in Aptio

The Aptio BIOS typically stores the passwords encrypted. For UEFI 2.1 BIOS, encryption is always used. The default encryption mechanism may be used; however, there is a hook in the BIOS project that allows for customization of the encryption mechanism. Thus, AMISCE has no way of reproducing the encryption of the BIOS password. However, AMISCE can still be used to replicate passwords on different systems.

Steps to setup a Password

The user can set a password through BIOS setup by following steps outlined below:

1. From BIOS Setup, set the desired password in a system.
2. Boot to an OS and use AMISCE (/o /n options) to extract the variable containing the password. This variable may be different for each BIOS, so the engineer responsible for the BIOS must provide this information. We recommend the use of a listing file ('/l' option) so that the script contains only the desired variable.
3. Use AMISCE (/i /n options) to install that password on other systems.



Note: AMISCE cannot decrypt the password; it is used to apply the password on other systems.

Example for changing Password without providing a Variable

Once the variable is extracted, the variable data corresponding to the particular variable name without inputting a password is displayed in the following format as outlined below,

```
Variable Name
AMITSESetup
Variable Data
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
```

To create a password, the user must change the variable data of the respective variable name, and install the password using the AMISCE in other systems. The below example shows a variable name with a password provided,

```
Variable Name
AMITSESetup
Variable Data
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 6A 93 87 26 20
BA 6C 4D C7 E0 22 74 7D 07 D8 9A 33 2E 8E C1 E9 54
44 E8 9F 7B FA 0E 55 A2 B0 35 0B C9 66 5C C1 EF 1C
83 00
```

Limitations

AMISCE does not have the encryption mechanism to support encryption. So AMISCE must rely on the BIOS setup such as AMITSE setup, to perform initial encryption. To make sure that the source and destination BIOS uses the same encryption method, set a password on each and verify that the variable has the same value. A possible source of differences is the TSE token for password case independence.

BIOS Configuration Requirements

The BIOS Configuration Requirements for AMISCE are outlined below,

- Aptio core version 5.008 for UEFI 2.3 and above
- Requires “SmiVariable” module to be present in the BIOS. The module can be found at:
Aptio V: `$/AptioV/Source/Modules/SmiVariable` labeled 5.004_SmiVariable_00 or later
Aptio 4: `$/Alaska/BIN/Modules/SmiVariable` labeled 4.6.3_SmiVariable_1.2 or later.
Note: AMISCE displays an error message and exits with an error code if the *SmiVariable* module is absent.
- For update of default values to be effective, the TSE module must be labeled 4.6.2_TSE_2_02_1205_BETA or later (for Aptio 4) and 5.004_AmiTse_13 or later (for Aptio V).
- Enable token ALWAYS_PUBLISH_HII_RESOURCES
- Requires ‘AmiSetupNvLock’ BIOS module for BIOS password check/change and NVRAM variable update protection. The module can be found at:
Aptio V: `$/AptioV/Source/Modules/AMISetupNVLock` labeled 5.004_AmiSetupNvLock_1_05 or later
Aptio 4: `$/Alaska/SOURCE/Modules/AMISetupNvLock` labeled 4.6.2_AmiSetupNvLock_1_02 or later
- If present, TSE token RT_ACCESS_SUPPORT_IN_HPKTOOL must be enabled.
- Bios version check requires:
ACPI label ‘ACPI_06’ or later for Aptio V.
ACPI label ‘4.6.5.0_ACPI_48’ or later for Aptio 4.
- SCE Linux under Xen (domain0 only) requires RuntimeMemoryHole Module.
- SCE for ARM Linux or EFI requires SceHiiInterface module in place of SmiVariable. Note that SceLnxArm does not require a Linux driver.
- Mapping language needs to be enabled for single question update from command line feature. The default mapping language x-AMI can be enabled by adding it to ‘RFC_LANGUAGES’ token value.
- For disable boot option support, TSE token TSE_SAVE_DISABLED_BBS_DEVICEPATH must be OFF. Otherwise, the change will be lost on next boot.
- For disable boot option support to work when FixedBootOrder module is present, Use label ‘FixedBootOrder_12’ or later.

The module can be found at:

AptioV: `$/AptioV/Source/Modules/BootOptionPolicies/FixedBootOrder`

Error and Warning Messages

AMISCE may give non-fatal warning messages. Warnings may be suppressed using the `/q` option in the command line. These are the most common:

1. **Warning in line nnnn
Missing Current Setting “*”**

Where nnnn is the line number of the input script where the error was detected. This is the first line of the setup question after the line that does not have the “*” character beside any of the option values. The user could have omitted the “*” when editing the script or the question did not have a value when the script was created.

2. **WARNING: Length of string for control (User Name) not updated as the value/defaults specified in the script file doesn't reach the minimum range (1).**

The string given in the script is shorter than the minimum length specified in the VFR for the control. The usual cause for this is that the string has an initial empty value. This and other similar warnings will cause import to exit with an error status when running with `/r` option.

3. **WARNING: Multiple instances of the setup question <Active Processor Cores> exist in the BIOS. The value for the duplicate instance of the question has not been modified (variable: Setup, GUID: ec87d643-eba4-4bb5-a1e5-3f3e36b20da, offset: 3a).**

In this example AMISCE has detected two or more controls with the same prompt “Active Processor Cores”. These are considered to be ambiguous for UEFI 2.0. This warning will not usually appear with a UEFI2.1 BIOS because the token ID is available to distinguish one control from another.

4. **Warning: HII data does not have setup question information.**

This usually means that the `ALWAYS_PUBLISH_HII_RESOURCES` token is not set to one. When this is the case, only partial HII data is available unless the user entered the operating environment from boot over ride.

5. **WARNING : Error in creating variable xxxxxxxx to NVRAM**

Where “xxxxxxx” is a variable name. This can happen when SCE attempts to create a missing variable from the copy of the variable within the `StdDefaults` variable. It will only try to do this if a value in the script differs from the default value. If the variable does not have the runtime attribute the write will fail if the variable is protected for security reasons. This warning commonly comes with the “`SecureBootEnable`” variable.

When AMISCE detects an error condition it will exit after printing the error. These are the likely errors:

1. Syntax Error in line 172

A Typographical error has occurred in the Setup question.

This error was generated by changing the keyword "Width" to "xWidth" on line number 172.

2. ERROR:4 - Retrieving HII Database

This error is usually caused by absence or old version of the SmiVariable module.

3. Platform identification failed

Indicates FIDT ACPI table could not be found. You may override this with '/d' option for Aptio V. Platform identification depends on ACPI module label 'ACPI_06' or later for Aptio V.

Linux/BSD Pre-Requisites (does not apply to ArmSceLnx)

1. Log in Linux as root otherwise use sudo (if permitted).
2. The compiler suite (gcc) must be installed. If these packages are not installed, the driver CANNOT be built.
3. For most of the distributions, SCE will generate driver without any notification, if it doesn't exist you need to install kernel sources. Also if `Initmem` fails, Please follow point 4.
4. Kernel sources must be installed, *CONFIGURED*, and then compiled. Following are steps to do this:

a. Find Running Kernel's Configuration File:

To configure the sources, simply change to the kernel source directory (typically `/lib/modules/$(uname -r)/build`). If it doesn't exist, you need to install kernel source. Typically, the reference configuration for the kernel can be found in the `/boot` directory with filename `'config'`, `'kernel.config'`, or `'vmlinuz-2.4.18-3.config'`. Type `'uname -a'` and use the configuration filename that best matches the output from `'uname -a'`. Also, check for `/dev/mem` directory existence. If it doesn't exist, you need to install kernel sources. Normally it comes with the installation unless if the option is deselected.

On some distributions Red Hat for instance, there is a config directory under `/lib/modules/$(uname -r)/build`.

Copy this configuration file into the root of the Linux kernel source tree (usually it is `/lib/modules/$(uname -r)/build`). This file must be renamed to `".config"`(dot config).

b. Make Your AMI Flash Driver (`amifldr_v mod.o`):

For most distribution, the command to build the driver is:

```
SCELNX_32 /MAKEDRV
Or
SCELNX_64/MAKEDRV
```

If your Linux's kernel source tree is under `/lib/modules/$(uname -r)/build`, instead of being in the default path `'/lib/modules/$(uname -r)/build'`, then add a KERNEL flag:

```
SCELNX_32 /MAKEDRV KERNEL=/lib/modules/$(uname -r)/build
Or
SCELNX_64 /MAKEDRV KERNEL=/lib/modules/$(uname -r)/build
```

If KERNEL is omitted, the default path is `/lib/modules/$(uname -r)/build`. This should work for MOST distributions.



Note: User should use `/MAKEDRV` to avoid building of the driver every time.

- C. Make Your AMI Flash Driver from driver source files (`amifldr_mod.o`):
Using command `/GENDRV`, it will generate driver source files to specific directory.
`AMISCE_32 /GENDRV [Option 1] [Option 2]`
Or
`AMISCE_64 /GENDRV [Option 1] [Option 2]`
Where,
[Option 1]: Specific kernel source 'KERNEL=XXXX' same as the `/MAKEDRV`
[Option 2]: Specific output directory 'OUTPUT=XXXX'

Generate files as outlined below:

File Name	Description

<code>amiwrap.c</code>	Driver source code.
<code>amiwrap.h</code>	Driver header.
<code>amifldr.o_shipped</code>	Object file for driver.
<code>Makefile</code>	Makefile

For most distribution, the command to build the driver is: `make`.

If your Linux's kernel source tree is under `/lib/modules/$(uname -r)/build`, instead of being in the default path `'/lib/modules/$(uname -r)/build'`, then add a KERNEL flag:

```
make KERNEL=/lib/modules/$(uname -r)/build
```

If KERNEL is omitted, the default is `/lib/modules/$(uname -r)/build`.
This should work for MOST distributions.

- d. Check Your Build:
Check the version of running Linux kernel with `'uname -r'`.
Check the version of `amifldr_mod.o` with `'modinfo amifldr_mod.o'`.

If they mismatch, you will need to select the correct configuration

File (.config), rebuild your kernel, and then rebuild your driver as described in steps a, b, c and d.

REFERENCES

Linux Loadable Kernel Module HOWTO

<http://www.linux.org/docs/ldp/howto/Module-HOWTO/index.html>

Signing Driver on RHEL 7 and Enrolling Public Key to the System

The following prerequisites are needed on the build system to sign the driver:

1. Login to RHEL 7 as root otherwise use sudo.
2. The compiler suite (gcc) must be installed. If it's not installed, the SCE driver cannot be built.
3. OpenSSL: Needed to generate cryptographic keys. OpenSSL tool can be downloaded from <https://www.openssl.org>
4. Perl interpreter: Needed to run the signing script. Perl tool can be downloaded from <https://www.perl.org>

Follow the below steps to sign the driver:

1. Boot to RHEL 7.
2. Generate a Public and Private key pair using below openssl command:

```
> openssl req -x509 -new -nodes -utf8 -sha256 -days 36500 -batch -config  
configuration_file.config -outform DER -out public_key.der -keyout private_key.priv
```

Note: The configuration file *configuration_file.config* must be created with the required information before running the command. A sample configuration file is shown below. The values in <> must be filled with actual values.

configuration_file.config:

```
[ req ]
default_bits = 4096
distinguished_name = req_distinguished_name
prompt = no
string_mask = utf8only
x509_extensions = myexts

[ req_distinguished_name ]
O = <organization_name>
CN = <organization_name> Signing Key
emailAddress = <email_address>

[ myexts ]
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```

3. Build SCE driver using below command. The driver will be generated in the current directory with name *amifldr_mod.o*.
 > *SCELNX_64 /MAKEDRV*
4. Execute below command to sign driver with the key generated in step 2.
 > *perl /usr/src/kernels/\$(uname -r)/scripts/sign-file sha256 private_key.priv public_key.der amifldr_mod.o*
5. Request addition of public key to MOK list using *mokutil*. The command will prompt a password which will be needed during public key enrollment in next step.
 > *mokutil --import public_key.der*
6. Reboot the system which will launch MOK manager application to complete public key enrollment.
7. Once the public key enrollment is done, Boot to OS and execute below command to ensure the newly added key is available in system key ring.
 > *keyctl list %:.system_keyring*
8. Install signed driver using *insmod* command.
 > *insmod amifldr_mod.o*
9. Ensure it is loaded successfully using *lsmod* command.

Reference: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/sect-signing-kernel-modules-for-secure-boot.html

SCE Exit Codes

Exit Code	Description
0x00	Operation completed successfully.
0x0D	Invalid script file or command line parameter.
0x17	Script file CRC check against current BIOS failed.
0x57	Incorrect command line usage.
0x86	Admin password does not exist.
0x82	Password does not match.
0x8F	Password retry count exceeded.
0x9A	Attempt to change password without providing current admin password.