

# SECURE BOOT CONFIGURATION INSTRUCTIONS FOR THE X12 MOTHERBOARDS

## **USER'S GUIDE**

Revision 1.0

The information in this user's guide has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this user's guide, or to notify any person or organization of the updates. Please Note: For the most up-to-date version of this user's guide, please see our website at www.supermicro. com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this user's guide at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING, OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in an industrial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

<u>California Best Management Practices Regulations for Perchlorate Materials</u>: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".



The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultraMay 07, 2021-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

User's Guide Revision 1.0

Release Date: May 07, 2021

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2021 by Super Micro Computer, Inc. All rights reserved. Printed in the United States of America

## Preface

## About This Manual

This user's guide is written for system integrators, IT technicians, and knowledgeable end users. It provides information on Secure Boot configuration in the UEFI BIOS Setup utility for Supermicro's X12 Series motherboards.

## **About This User's Guide**

This user's guide provides detailed instructions on how to configure Secure Boot settings in the UEFI BIOS for the X12 motherboards that are based on the 3rd Gen Intel® Xeon® Scalable Processors. Please note that all Supermicro's products are intended to be installed, configured, and serviced by professional technicians only.

For processor/memory updates, please refer to our website at http://www.supermicro.com/ products/.

## **Conventions Used in the Manual**

Special attention should be given to the symbol below for proper BIOS configuration and for prevention of accidental damage to your system components:

**Note:** Important Information given for proper system setup or for proper firmware configuration.

#### Contacting Supermicro

Headquarters	
Address:	Super Micro Computer, Inc.
	980 Rock Ave.
	San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information)
	support@supermicro.com (Technical Support)
Website:	www.supermicro.com
Europa	
Europe Address:	Super Micro Computer B.V.
Address.	Het Sterrenbeeld 28, 5215 ML
	's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information)
Lindii.	support@supermicro.nl (Technical Support)
	rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl
Asia-Pacific	
Address:	Super Micro Computer, Inc.
	3F, No. 150, Jian 1st Rd.
	Zhonghe Dist., New Taipei City 235
	Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

## **Table of Contents**

#### Preface

## Configuring Secure Boot Settings

Section 1 Setting Your Boot Mode to UEFI	6
Section 2 Secure Boot/Secure Boot Mode/CSM Support	7
Section 3 Secure Boot Settings	8
Section 4 Key Management Settings	.11
Important keys and signatures used in Secure Boot	.15

## **Configuring Secure Boot Settings**

Secure Boot, a feature available in the Unified Extensible Firmware Interface (UEFI) BIOS, supports Secure Boot by preventing drivers and OS loaders from booting up without an acceptable digital signature. Secure Boot ensures that boot loaders are digitally signed and validated upon system boot. It is imperative that Secure Boot settings be properly configured prior to using your machine. Sections 1~3 of this document provide instructions on how to enable the Secure Boot features in UEFI. Section 4 provides information on how to configure Key Management settings. To configure your BIOS settings for Secure Boot, please follow the instructions below.

## Section 1 Setting Your Boot Mode to UEFI

Since Secure Boot is a feature of UEFI, you will need to enable Secure Boot mode in the UEFI first by following the steps below.

- 1. Press <Del> during system boot to enter the BIOS Setup utility.
- 2. Select the Boot tab from the menu bar on the top of the screen and press <Enter>. Using the down arrow key, scroll down to select the feature: Boot Mode Select and press <Enter>.
- 3. The Boot Mode Select setting options, which include LEGACY, UEFI, and DUAL, will display as shown in the screen below. From the Boot options, select UEFI and press <Enter> to set Boot mode to UEFI.
- 4. For the changes to take effect, press <F4> to save the setting and reboot the system.



## Section 2 Secure Boot/Secure Boot Mode/CSM Support

To use the Secure Boot feature, you will need to have a set of platform key (PK) pre-registered in the platform on which your system is operating. You will also need to enable the Secure Boot feature, set Secure Boot mode to Custom, and disable CMS support in the BIOS Setup utility. To do so, please follow the instructions below:

Press <Del> upon system boot to enter the BIOS Setup. Select Security from the top menu bar.

Main Advanced Event Logs IF	Aptio Setup – AMI MI Security Boot Save &	8 Exit
If the Administrator's / User's then this only limits access to asked for when entering Setup. Please set Administrator's pass to set User's password, if clea password, the User's password w	Setup and is word first in order r Administrator's	▲ Secure Boot configuration
The password length must be		
in the following range:		
Minimum length	3	
Maximum length	20	
Administrator Password Password Check SATA Frozen	[Setup] [Enabled]	++: Select Screen 14: Select Item Enter: Select
▶ SMC Security Erase Configuratio	n	+/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
HDD Security Configuration: P4:WDC WD800JD-00MSA1		ESC: Exit
▶ Secure Boot		
Vers	ion 2.21.1280 Copyright (C	C) 2021 AMI

When the screen above displays, select Secure Boot and press <Enter> to access the menu items. The following screen will appear.



## **Section 3 Secure Boot Settings**

To properly configure the Secure Boot settings, please follow the steps below.

Step 1. Set Secure Boot Mode to Standard. Press Yes to install the manufacturer default keys as needed.

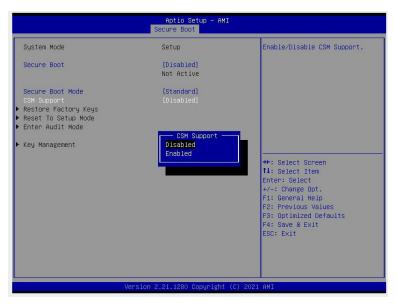
System Mode	Setup	Secure Boot mode options:
Secure Boot	[Disabled] Not Active	Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically
Secure Boot Mode	[Standard]	present user without full
usm support Restore Factory Keys Reset To Setup Mode Enter Audit Mode	[01580180]	authentication
Key Management	Secure Boot Mode - Standard Dustom	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

**Note:** The Key Management menu will not be available when Secure Boot Mode is set to Standard.

Step 2. For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

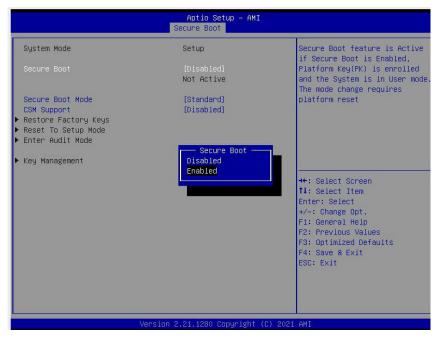


Step 3. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab to enter the Secure Boot menu. Set CSM Support to Disabled as mentioned in Section 1.



For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

Step 4. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. Set Secure Boot to Enabled.



For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. The following screen will appear.

Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc. Security			
System Mode Vendor Keys Secure Boot	User Active Active	Secure Boot feature is Active if Secure Boot is Enabled,	
Secure Boot Secure Boot Mode CSM Support	[Enabled] [Standard] [Disabled]	Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset	
▶ Key Management			
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.20.1274.	Copyright (C) 2019 Americ:	an Megatrends, Inc.	

**Note:** Once Secure Boot is enabled, CSM Support will become disabled and the legacy platform will no longer supported; only the authorized UEFI applications such as UEFI OS, AOC UEFI FW, and UEFI PXE server will be allowed in the platform.

### **Section 4 Key Management Settings**

The Key Management menu, which is only available when Secure Boot Mode is set to Custom, allows Secure Boot keys to be installed via an external device and to be used for secure system boot.

	Key Management	
Vendor Keys	Valid	Install factory default Secure Boot keys after the platform
Factory Key Provision • Restore Factory Keys • Reset To Setup Mode • Export Secure Boot variables • Enroll Efi Image • Device Guard Ready • Remove 'UEFI CA' from DB • Restore DB defaults		reset and while the System is in Setup mode
Secure Boot variable   Size   H Platform Key(PK)   862  Key Exchange Keys   1560  Authorized Signatures   4269  Forbidden Signatures   3724  Authorized TimeStamps   0  OsRecovery Signatures   0	1  Test(AMI) 1  Factory 3  Factory 77  Factory	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>

#### **Vendor Keys**

#### **Factory Key Provision Defaults**

This feature is used to provision the default Secure Boot keys pre-set by the manufacturer when system is in Setup mode. Select **Disabled** to use your own Secure Boot keys for system boot.

Vendor Keys	Valid	Install factory default Secure Boot keys after the platform
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image		reset and while the System is in Setup mode
Device Guard Ready • Remove 'UEFI CA' from DB • Restore DB defaults		
• Authorized TimeStamps  0	1  Test(AMI) 1  Factory 3  Factory 77  Factory	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

#### ► Restore Factory Keys

Select Yes and press <Enter> to restore the manufacturer default Secure Boot keys. This will also reset the system to User mode. The options are **Yes** and No.

Vendor Keys	Valid		arce System to User Mode. Istall factory default Secure
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot varia Enroll Efi Image	(Disabled) ables		starr factory default secure
Device Guard Ready			
Remove 'UEFI CA' from DI	B Install factor	ry defaults ———	
Restore DB defaults	Press 'Yes' to procee	d Not to concol	
Secure Boot variable   :	Siz	su NU (U CANCEI	
Platform Key(PK)	86		elect Screen
	156 Yes	No	elect Item
and the second sec	126		: Select
Authorized Signatures			
Forbidden Signatures	3724		Change Opt.
Authorized Signatures   - Forbidden Signatures   : Authorized TimeStamps	3724  0  0  No Keys		l: General Help
Forbidden Signatures  : Authorized TimeStamps		Fa	l: General Help 2: Previous Values
Forbidden Signatures  : Authorized TimeStamps	0  0  No Keys	F6 F0	l: General Help 2: Previous Values 3: Optimized Defaults
Forbidden Signatures  : Authorized TimeStamps	0  0  No Keys	F: F: F:	I: General Help 2: Previous Values 3: Optimized Defaults 4: Save & Exit
Forbidden Signatures  : Authorized TimeStamps	0  0  No Keys	F: F: F:	l: General Help 2: Previous Values 3: Optimized Defaults
Forbidden Signatures  : Authorized TimeStamps	0  0  No Keys	F: F: F:	I: General Help 2: Previous Values 3: Optimized Defaults 4: Save & Exit
Forbidden Signatures  : Authorized TimeStamps	0  0  No Keys	F: F: F:	I: General Help 2: Previous Values 3: Optimized Defaults 4: Save & Exit
Forbidden Signatures	0  0  No Keys	F: F: F:	I: General Help 2: Previous Values 3: Optimized Defaults 4: Save & Exit

# ▶ Reset To Setup Mode (Available when the System Mode is in User mode)

Select Yes and press <Enter> to clear all Secure Boot values and reset the system to Setup mode. The options are **Yes** and No.

	Aptio Setu Key Managemer		
Vendor Keys Factory Key Provision ▶ Resetore Factory Keys ▶ Reset To Setup Mode ▶ Export Secure Boot variables ▶ Enroll Efi Image	Valid (Disabled)		Delete all Secure Boot key databases from NVRAM
Device Guand Ready > Remove 'UEFI CA' from DB > Restore DB defaults Secure Boot variable   Siz > Platform Key(PK)   B6 > Key Exchange Keys   156 > Authorized Signatures  426 > Forbidden Signatures  372 > Authorized TimeStamps  0 > DsRecovery Signatures  0	Deleting all variab System to Sa Do you want f Yes	Change Opt. eneral Help	
	/ersion 2.21.1280 Co	pyright (C) 2021	AMI

#### **Export Secure Boot Variables**

Use this feature to export the Secure Boot values to the files in a root folder that resides in a file system device.

Vendor Keys	Valid	Copy NVRAM content of Secure Boot variables to files in a
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	root folder on a file system device
Device Guard Ready Re Re	Select a File syst	
		ype i)HD(Parti, Sig −WMAM9DYD9568)∖ –
Pl Key Exchange Keys   1560  Authorized Signatures  4269	1  Factory 3  Factory	t↓: Select Item Enter: Select
Forbidden Signatures 3724 Authorized TimeStamps 0	77  Factory 0  No Keys	+/-: Change Opt. F1: General Help
OsRecovery Signatures   0	0  No Keys	F2: Previous Values F3: Optimized Defaults F4: Save & Exit

### ►Enroll Efi Image

This feature enrolls SHA256 hash binary data in the Authorized Signature Database (DB) and allows the image to run in Secure Boot mode.

Secure Boot mode. Enroll SHA256 Hash certificat of a PE image into Authorized Signature Database (db)
arti, Sig –WMAM9DYD9568)\
t↓: Select Item
Enter: Select
+/−: Change Opt.
F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
H H

#### **Device Guard Ready**

# ▶ Remove 'UEFI CA' from DB (Database) (available when the system is not in Device Guard Ready)

Select Yes and press <Enter> to remove the Microsoft UEFI CA certificate from the database (DB). The options are **Yes** and No.

Aptio Setup – AMI Key Management				
Vendor Keys Factory Key Provision • Restore Factory Keys • Reset To Setup Mode • Export Secure Boot variable • Enroll Efi Image Device Guard Ready • Remove 'UEFI CA' from DB • Restore DB defaults	Valid [Disabled]	no Ce Si from DB	vice Guard ready system must t list 'Microsoft UEFI CA' rtificate in Authorized gnature database (db)	
	Yes	No F1 F2 F3 F4	elect Screen elect Item : Select Change Opt. : General Help : Previous Values : Optimized Defaults : Save & Exit C: Exit	

#### ► Restore DB (Database) defaults

Select Yes and press <Enter> to restore the DB variables to the manufacturer default settings. The options are **Yes** and No.

	Aptio Setu Key Managemer		
Vendor Keys Factory Key Provision > Restore Factory Keys > Reset To Setup Mode > Export Secure Boot variab > Ennoll Efi Image	Valid [Disabled] les		Restore DB variable to factory defaults
Device Guand Ready Remove 'UEFI CA' from DB Restore DB defaults Secure Boot variable   Si Platform Key(PK)   8 Key Exchange Keys   15 Authorized Signatures   37 Authorized TimeStamps OsRecovery Signatures	6 Yes	eed 'No' to cance No	elect Screen elect Item : Select Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.21.1280 Cop	yright (C) 2021	AMI

#### Important keys and signatures used in Secure Boot

#### ► Platform Key (PK)

The Platform Key (PK), which is pre-installed in the system firmware during manufacturing, provides the full control of key hierarchy in Secure Boot. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load PKs from a file in an external device. Select Delete to clear the current PKs and reset the system to Setup mode. See the following screen for more information.

	Aptio Setup – AMI Key Management	
Vendor Keys	Modified	Enroll Factory Defaults or
Factory Key Provision ► Restore Factory Keys ► Reset To Setup Mode ► Export Secure Boot variables ► Enroll Efi Image	(Disabled)	<pre>load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable</pre>
Device Guard Ready	Platform Key(PK)	3.EFI PE/COFF Image(SHA256)
<ul> <li>Remove 'UEFI CA' from DB</li> <li>Restore DB defaults</li> </ul>	Details Export	- Key Source: Factory,External,Mixed
Secure Boot variable   Size  Kı ▶ Platform Key(PK)   862	e Update Delete	++: Select Screen
<ul> <li>Key Exchange Keys   1560  </li> <li>Authorized Signatures   4269  </li> </ul>	3  Factory	↓ 11: Select Item Enter: Select
<ul> <li>Forbidden Signatures 3724</li> </ul>	77  Factory	+/-: Change Opt.
► Authorized TimeStamps  0	0  No Keys	F1: General Help
▶ OsRecovery Signatures  0	0  No Keys	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Ven	sion 2.21.1280 Copyright (C) 202	21 AMI

**Details**: Use the arrow keys to select **Details** (default) and press <Enter>. This displays detailed information of PK as shown below.

Vendor Keys			Modified	Enroll Factory Defaults or load certificates from a file:
Enroll Efi	tory Keys tup Mode re Boot vari Image	ables	[Disabled]	1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variable
Device Guar Remove 'UEF			Platform Key(PK)	e(SHA256)
Restore DB				ixed
Restore DB	List  Sig.		t  Size  Owner GUID   1  818  26DC4851	Certificate Legend
Restore DB Secure Boot Platform Ke Key Exchang	List  Sig. 1  X.5 e Keys	09   1560	t  Size  Owner GUID   1  818  26DC4851  1  Factory	Certificate Legend DO NOT TRUST - AMI Test PK 11: Select Item
Restore DB Secure Boot Platform Ke Key Exchang Authorized	List  Sig. 1  X.5 e Keys   Signatures	09   1560   4269   3	t  Size  Owner GUID   1  818  26DC4851  1  Factory 3  Factory	Certificate Legend DO NOT TRUST - AMI Test PK 11: Select Item Enter: Select
Restore DB Secure Boot Platform Ke Key Exchang Authorized Forbidden	List  Sig. 1  X.5 e Keys	09   1560   4269   3 3724   7	t  Size  Owner GUID   1  818  26DC4851  1  Factory	Certificate Legend DO NOT TRUST - AMI Test PK 11: Select Item

**Export**: Use the arrow keys to select Export and press <Enter>. This option saves the current PKs to a FAT-formatted USB flash drive.

Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a file:
Factory Key Provision • Restore Factory Keys • Reset To Setup Mode • Export Secure Boot variable: • Enroll Efi Image	[Disabled]	1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_SA2040 (bin) d)EFI_CERT_SHAXXX
Device Guard Ready	Platform Key(PK)	2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256)
• Remove 'UEFI CA' from DB		Key Source:
Restore DB defaults Secure Boot variable   Size	Details Export Ke Update	Factory,External,Mixed
▶ Platform Key(PK)   862		++: Select Screen
Key Exchange Keys   1560	2 Contraction of the second seco	↑↓: Select Item
Authorized Signatures  4269	3  Factory	Enter: Select
Forbidden Signatures  3724		+/-: Change Opt.
<ul> <li>Authorized TimeStamps  0</li> </ul>		F1: General Help
⊳ OsRecovery Signatures  0	0  No Keys	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Press <Enter> and the following screen will appear.

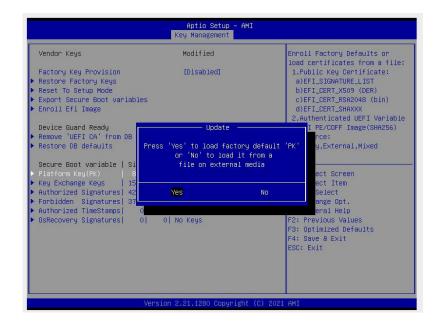
Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a file
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variable Enroll Efi Image Device Guard Ready	[Disabled] es	<pre>load certificates from a file 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_R5A2046 (bin) d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variabl 3.EFI PE/COFF Image (SH4256)</pre>
Re		S.EFT FE, SOFT INdectormesoy
Re	Select a File sys	tem
Key Exchange Keys   1560 Authorized Signatures  4269	3  3  Factory	1↓: Select Item Enter: Select
Forbidden Signatures 3724 Authorized TimeStamps (		+/-: Change Opt. F1: General Help
	)  O  No Keys )  O  No Keys	F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
		ESC: Exit

**Note:** Refer to the right panel of the screen to display the file formats that are supported by your platform.

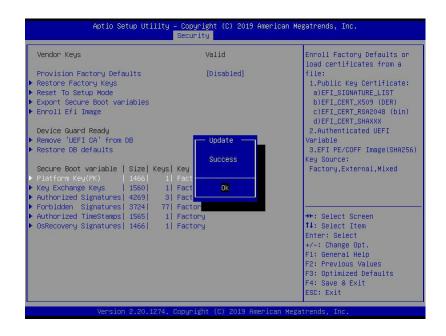
**Update**: Use the arrow keys to select Update. This will load the manufacturer defaults or load PKs from a file in an external device.

Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a file
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_R5A2040 (bin) d)EFI_CERT_SHAXXX
Device Guard Ready	Platform Key(PK)	2.Authenticated UEFI Variabl 3.EFI PE/COFF Image(SHA256)
Remove 'UEFI CA' from DB		Key Source:
Restore DB defaults Secure Boot variable   Size	Details Export Ke Update	Factory,External,Mixed
Platform Key(PK)   862	Delete	++: Select Screen
Key Exchange Keys   1560		t∔: Select Item
- Authorized Signatures  4269  - Forbidden Signatures  3724	3  Factory	Enter: Select
• Authorized TimeStamps  0	77  Factory 0  No Keys	+/-: Change Opt. F1: General Help
OSRecovery Signatures  0	Oļ No Keys	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Press <Enter> and the following screen will appear.



To load the manufacturer defaults, select Yes and press <Enter>. The following screen will appear.



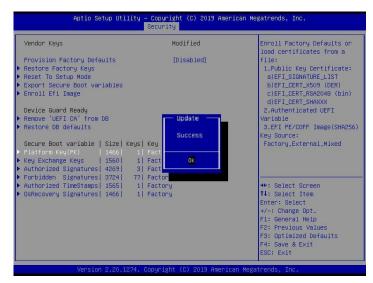
To load PKs from a file in an external device, select No and press <Enter>.

Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a
Provision Factory Defaults	[Disabled]	file:
Restore Factory Keys	[0 1000 1003]	1.Public Key Certificate:
Reset To Setup Mode		a)EFI_SIGNATURE_LIST
Export Secure Boot variables		b)EFI_CERT_X509 (DER)
Enroll Efi Image		c)EFI_CERT_RSA2048 (bin)
		d)EFI_CERT_SHAXXX
Device Guard Ready	Update	.Authenticated UEFI
Remove 'UEFI CA' from DB		able
Restore DB defaults Pre	ss 'Yes' to load factory default 'F	and a second sec
	or 'No' to load it from a	Source:
Secure Boot variable   Si	file on external media	tory,External,Mixed
Platform Key(PK)   14 Key Exchange Keys   15		
Key Exchange Keys   15 Authorized Signatures  42	Yes No	
Forbidden Signatures 37		
Authorized TimeStamps  1565		Select Screen
OsRecovery Signatures   1466	1  Factory	↑↓: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit ESC: Exit
		F1: General Help F2: Previous Values

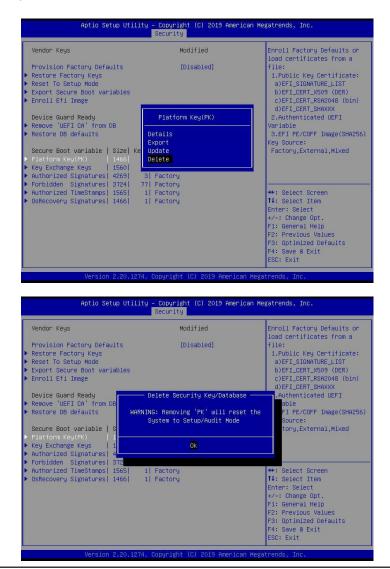
When the following screens appear, select the USB flash drive that contains the desired file and press <Enter>.



Press <Enter> and the following screen will appear.



Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to Setup mode.



#### ► Key Exchange Key

The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and is used in Secure Boot to protect the data base that contains signatures from being illegal accessed. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of KEKs. Select Export to save the current KEKs to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load KEKs from a file in an external device. Select Delete to clear the current KEKs or to delete only one certificate from the key database. (Refer to page 16 for the Export process. Refer to pages 17, 18, 21 and 22 for the Update process.)

Vendor Keys	Modified	Enroll Factory Defaults or
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	<pre>load certificates from a file 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_SHAXXX d)EFI_CERT_SHAXXX 2.Authenticated UEFI Variabl</pre>
Device Guard Ready Remove 'UEFI CA' from DB	Key Exchange Keys	3.EFI PE/COFF Image(SHA256)
Restore DB defaults Secure Boot variable   Size  Ki Platform Key(PK)   662  Key Exchange Keys   1560  Authorized Signatures  4269  Forbidden Signatures  4269  Authorized TimeStamps  0  OsRecovery Signatures  0	Details Export Update Append Delete 77  Factory 0  No Keys 0  No Keys	Key Source: Factory,External,Mixed +: Select Scneen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

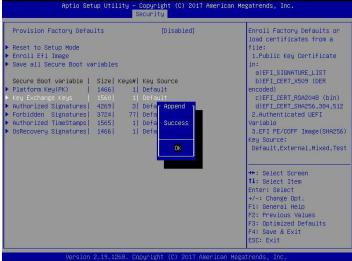
Append: Use the arrow keys to select Append.

Vendor Keys	Modified	Enroll Factory Defaults or
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	<pre>load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_X509 (Din) d)EFI_CERT_SHAXXX</pre>
Device Guard Ready	Key Exchange Keys	2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256)
Remove 'HEET CA' from DB		Key Source:
Restore DB defaults	Details Export	Factory,External,Mixed
Secure Boot variable   Size	Ke Update	
Platform Key(PK)   862	Append	++: Select Screen
	Delete	1↓: Select Item
Authorized Signatures   4269		Enter: Select
Forbidden Signatures   3724	77  Factory	+/-: Change Opt.
Authorized TimeStamps  0	0  No Keys	F1: General Help
OsRecovery Signatures  0	0  No Keys	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Press <Enter> and the following screen will appear.

Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a file
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot varial Enroll Efi Image	[Disabled] Dies	1.Fublic Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_K509 (DER) d)EFI_CERT_SHAXXX 2.Authenticated UEFI variabl
Device Guard Ready	Append -	I PE/COFF Image(SHA256)
Remove 'UEFI CA' from DB		rce:
Restore DB defaults Secure Boot variable   S Platform Key(PK)   Key Exchange Keys   1	Press 'Yes' to load factory or 'No' to load it file on external	from a
Authorized Signatures 4	Yes	No
Forbidden Signatures  3		ange Opt.
	0  0  No Keys	eral Help F2: Previous Values
Authorized TimeStamps  OsRecovery Signatures		

To load the manufacturer defaults, select Yes and press <Enter>. The following screen will appear.



To load KEKs from a file in an external device, select to No and press <Enter>. Refer to pages 21 and 22 on how to load KEKs from a file in an external device.

Vendor Keys	Modified		Enroll Factory Defaults or load certificates from a
Provision Factory Defaults Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]		<pre>file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_RSA2048 (bin)</pre>
Device Guard Ready Remove 'UEFI CA' from DB Restore DB defaults Secure Boot variable   S Platform Key(PK)   1	Append — s 'Yes' to load factory or 'No' to load it file on external	from a	<pre>d) EFI_CERT_SHAXXX .Authenticated UEFI able FI PE/COFF Image(SHA256 Source: tory,External,Mixed</pre>
· Flattorm Key(PK)   1 · Key Exchange Keys   1 · Authorized Signatures  4 · Forbidden Signatures  3	Yes	No	
- Authorized TimeStamps  156 - OsRecovery Signatures  1466	1  Factory		Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit F4: Save & Exit F50: Exit

Delete: Use the arrow keys to select Delete and press <Enter>. Select Yes and press <Enter> to clear the current KEKs.

Vendor Keys	Modified	Enroll Factory Defaults or
Factory Key Provision • Restore Factory Keys • Reset To Setup Mode • Export Secure Boot variables • Enroll Efi Image	[Disabled]	<pre>load certificates from a file 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_X509 (DER) d)EFI_CERT_SHAXXX</pre>
Device Guard Ready	Key Exchange Keys	2.Authenticated UEFI Variable 3.EFI PE/COFF Image(SHA256)
Remove 'UEFI CA' from DB Restore DB defaults	Details	Key Source: Factory,External,Mixed
	Export	ractor 312ntor naziminos
Secure Boot variable   Size  Ke		
▶ Platform Key(PK)   0  ▶ Key Exchange Keys   1560	Append Delete	<pre>++: Select Screen  f↓: Select Item</pre>
Authorized Signatures   4269		Enter: Select
	77  Factory	+/-: Change Opt.
Authorized TimeStamps  0	0  No Keys	F1: General Help
OsRecovery Signatures  0	0  No Keys	F2: Previous Values F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit

Vendor Keys	Modified		Factory Defaults or	
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot vari: Enroll Efi Image	(Disabled) ables	1.Put a)EF b)EF c)EF d)EF	<pre>load certificates from a file: 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER) c)EFI_CERT_SHA2XA d)EFI_CERT_SHAXXA 2.Authenticated UEFI Variable</pre>	
Device Guard Ready	Delete Security K	ey/Database ————	PE/COFF Image(SHA256)	
Remove 'UEFI CA' from D Restore DB defaults Secure Boot variable   : Platform Key(PK)	Press 'Yes' to delete t 'No' to delete only a cer Key databa	tificate from the	rce: y,External,Mixed ect Screen	
Key Exchange Keys	1 Ves	No	ect Item Select	
Authorized Signatures		NU	ange Opt.	
Authorized TimeStamps  OsRecovery Signatures  0	0  0  No Keys	F3: Op	eral Help revious Values otimized Defaults ave & Exit	

Select No and press <Enter> to delete only one certificate from the key database.

Vendor Keys	Modified	Enroll Factory Defaults or load certificates from a fil
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variable Enroll Efi Image	[Disabled] s	1.Public Key Certificate: a)EFL_SIGNATURE_LIST b)EFL_CERT_XS09 (DER) c)EFL_CERT_XS09 (DER) d)EFL_CERT_SN9408 (bin) d)EFL_CERT_SN94XXX 2.Authenticated UEFI Variat
Device Remove Select a	Signature List to be removed	d from a key database
		rosoft Corporation KEK CA 2011
Key Exchange Keys   1560 Authorized Signatures   4269		14: Select Item Enter: Select
Authorized Signatures  4269 Forbidden Signatures  3724	3  Factory   77  Factory	Enter: Select +/-: Change Opt.
Authorized Signatures  4269	3  Factory   77  Factory   0  No Keys	Enter: Select

#### ► Authorized Signatures

Authorized Signature Database (DB) contains authorized signing certificates and digital signatures. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Authorized Signatures. Select Export to save the current DB to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load DB from a file in an external device. Select Append to add variables to the existing DB. Select Delete to clear the current DB or to delete only one certificate from the key database. (Refer to page 16 for the Export process. Refer to pages 17, 18, 19, and 20 for the Update process. Refer to pages 21 and 22 for the Append process. Refer to page 23 for the Delete process.)



#### ► Forbidden Signatures

Forbidden Signature Database (DBX) contains forbidden certificates and digital signatures. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Forbidden Signatures. Select Export to save the current DBX to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load DBX from a file in an external device. Select Append to add variables to the existing DBX. Select Delete to clear the current DBX or to delete only one certificate from the key database. (Refer to page 16 for the Export process. Refer to pages 17, 18, 19, and 20 for the Update process. Refer to pages 21 and 22 for the Append process. Refer to page 23 for the Delete process.)

Vendor Keys	Modified	Enroll Factory Defaults or
Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image	[Disabled]	<pre>load certificates from a file 1.Public Key Certificate: a)EFI_SIGNATURE_LIST b)EFI_CERT_XSO9 (DER) c)EFI_CERT_XSO9 (DER) d)EFI_CERT_SHAXXX</pre>
Device Guard Ready Remove 'UEFI CA' from DB Restore DB defaults	Forbidden Signatures Details Export	2.Authenticated UEFI Variabl 3.EFI PE/COFF Image(SHA256) Key Source: Factory,External,Mixed
Secure Boot variable   Size  K Platform Key(PK)   0  Key Exchange Keys   1560  Authorized Signatures   3724  Forbidden Signatures   3724	e Update Append Delete 77  Factory	++: Select Screen 14: Select Item Enter: Select +/-: Change Opt.
Authorized TimeStamps  0  OsRecovery Signatures  0	0  Na Keys 0  Na Keys	Fi: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

#### ► Authorized TimeStamps

Authorized Timestamp Database (DBT) issues and checks signed timestamp certificates. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Authorized timestamps. Select Export to save the current DBT to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load DBT from a file in an external device. Select Append to add variables to the existing DBT. Select Delete to clear the current DBT or to delete only one certificate from the key database. (Refer to page 16 for the Export process. Refer to pages 17, 18, 19, and 20 for the Update process. Refer to pages 21 and 22 for the Append process. Refer to page 23 for the Delete process.)

Provision Factory Defaults	[Disabled]	Enroll Factory Defaults or load certificates from a
<ul> <li>Reset to Setup Mode</li> <li>Enroll Efi Image</li> </ul>		file: 1.Public Key Certificate
· Save all Secure Boot variables		in:
Secure Boot variable   Size  Keys#	Key Source	a)EFI_SIGNATURE_LIST b)EFI_CERT_X509 (DER
Platform Key(PK)   1466  Key Exchange Keys   1560	Key Management	encoded) c)EFI CERT RSA2048 (bin)
Authorized Signatures  4269		d)EFI_CERT_SHA256,384,51
• Forbidden Signatures  3724  7 • Authorized TimeStamps  1565	Save to File Set New	2.Authenticated UEFI Variable
OsRecovery Signatures  1466	Append Erase	3.EFI PE/COFF Image(SHA25 Key Source:
	Erase	Default,External,Mixed,Te
		++: Select Screen
		14: Select Item Enter: Select
		+/-: Change Opt.
		F1: General Help F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit ESC: Exit

#### ► OsRecovery Signatures

OsRecovery Signatures Database (DBR) contains recovery variables that are authorized by Secure Boot. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of OsRecovery Signatures. Select Export to save the current DBR to a FAT-formatted USB flash drive. Select Update to load the manufacturer defaults or load DBR from a file in an external device. Select Append to add variables to the existing DBR. Select Delete to clear the current DBR or to delete only one certificate from the key database. (Refer to page 16 for the Export process. Refer to pages 17, 18, 19, and 20 for the Update process. Refer to pages 21 and 22 for the Append process. Refer to page 23 for the Delete process.)

Provision Factory Defaults	[Disabled]	Enroll Factory Defaults or load certificates from a
Reset to Setup Mode		file:
· Enroll Efi Image · Save all Secure Boot variables		1.Public Key Certificate
Save all secure boot variables		a)EFI_SIGNATURE_LIST
Secure Boot variable   Size  Keys	#  Key Source	b)EFI_CERT_X509 (DER
Platform Key(PK)   1466		encoded)
Key Exchange Keys   1560  Authorized Signatures  4269	Key Management	<pre>c)EFI_CERT_RSA2048 (bin) d)EFI_CERT_SHA256.384.512</pre>
Forbidden Signatures  3724  7		2.Authenticated UEFI
Authorized TimeStamps  1565	Set New	Variable
	Append Erase	3.EFI PE/COFF Image(SHA256 Key Source:
		Default,External,Mixed,Tes
		++: Select Screen
		↑↓: Select Item
		Enter: Select
		+/-: Change Opt. F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit ESC: Exit