



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.**

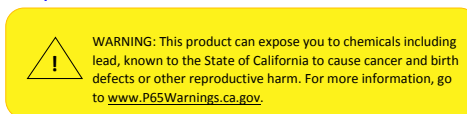
Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this user's guide at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any 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.

California Best Management Practices Regulations for Perchlorate Materials: 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

Europe

Address: Super Micro Computer B.V.
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)
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

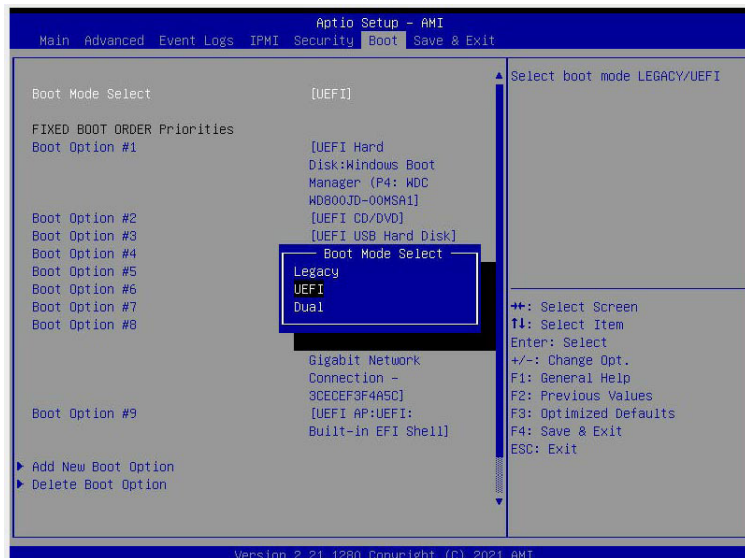
Configuring Secure Boot Settings

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.

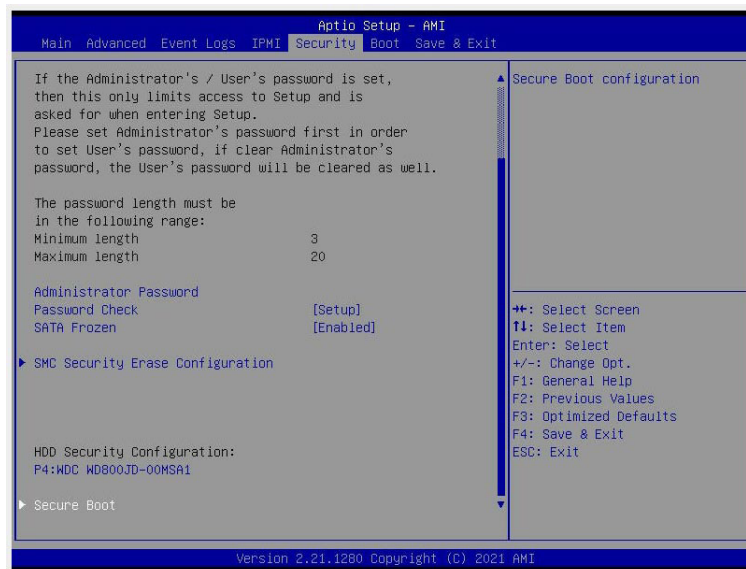
1. Press during system boot to enter the BIOS Setup utility.
2. Select the Boot tab from the menu bar on the top of the screen and press <Enter>. Using the down arrow key, scroll down to select the feature: Boot Mode Select and press <Enter>.
3. The Boot Mode Select setting options, which include LEGACY, 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.



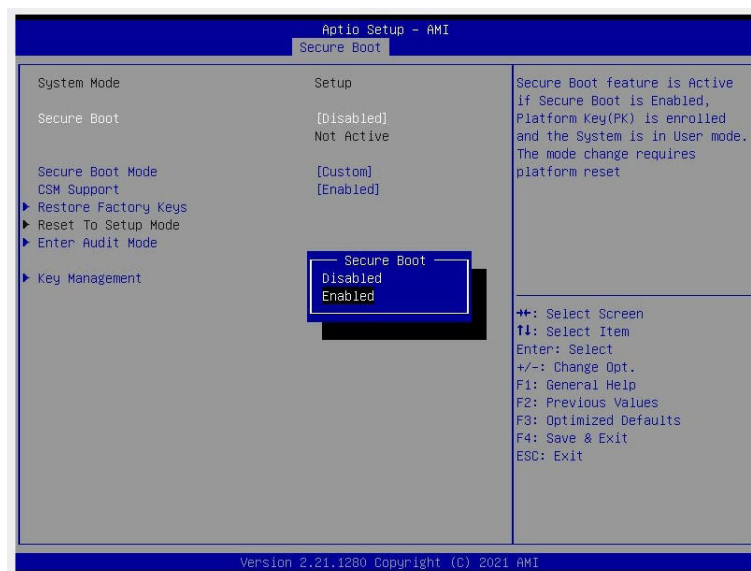
Section 2 Secure Boot/Secure Boot Mode/CSM Support

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 upon system boot to enter the BIOS Setup. Select Security from the top menu bar.



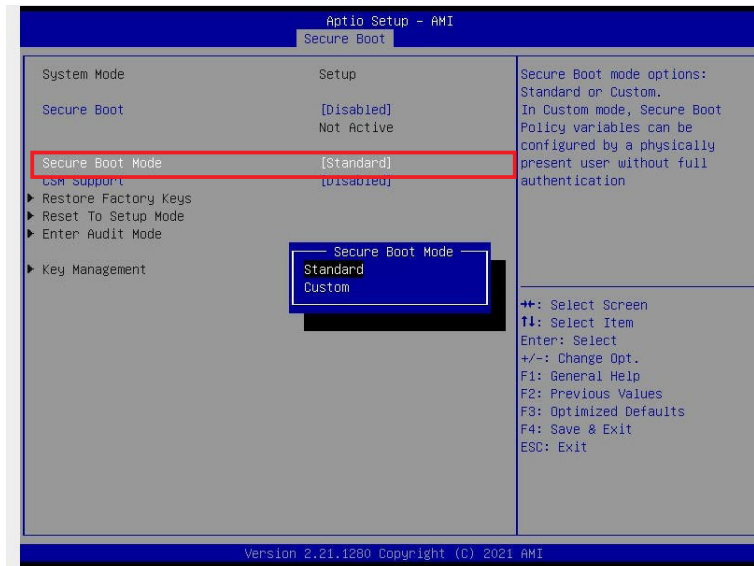
When the screen above displays, select Secure Boot and press <Enter> to access the menu items. The following screen will appear.




Section 3 Secure Boot Settings

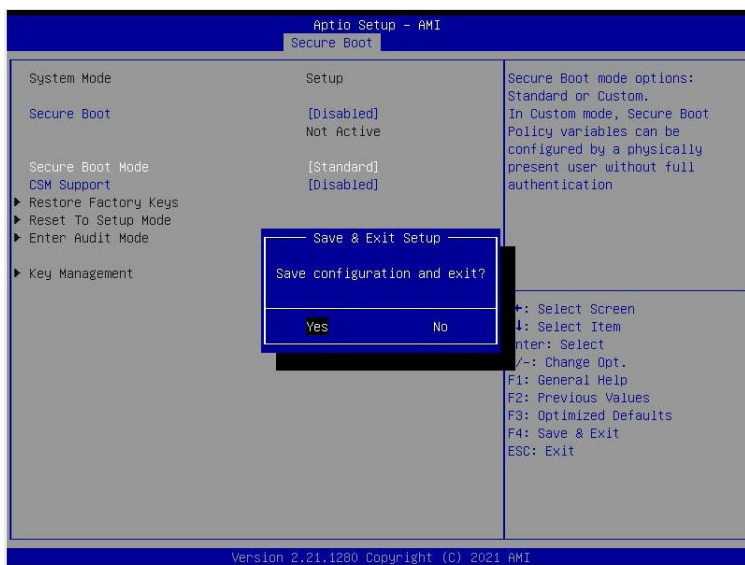
To properly configure the Secure Boot settings, please follow the steps below.

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

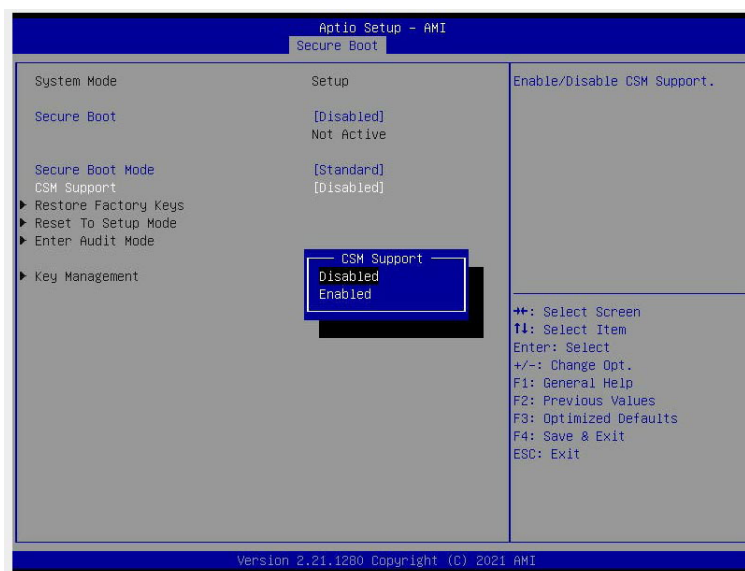


 **Note:** The Key Management menu will not be available when Secure Boot Mode is set to Standard.

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



Step 3. Press 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.

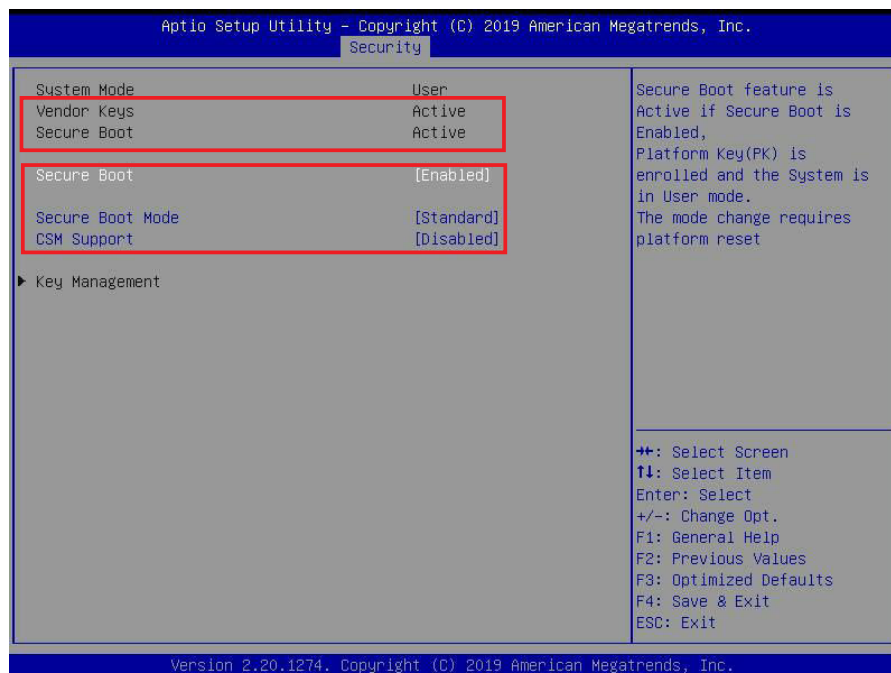


For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

Step 4. Press 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 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.



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

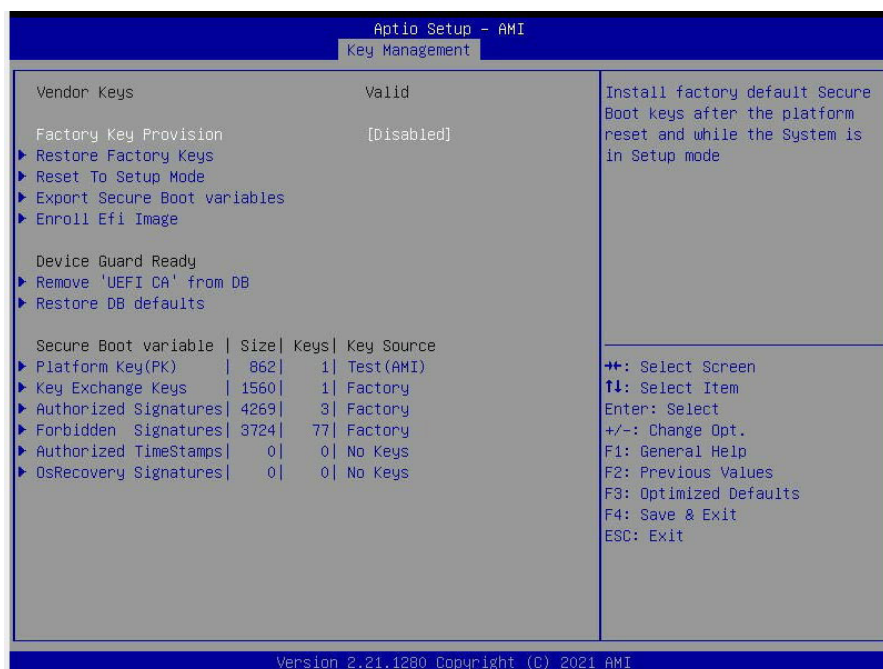
The Key Management menu, which is only available when Secure Boot Mode is set to Custom, allows Secure Boot keys to be installed via an external device and to be used for secure system boot.



Vendor Keys

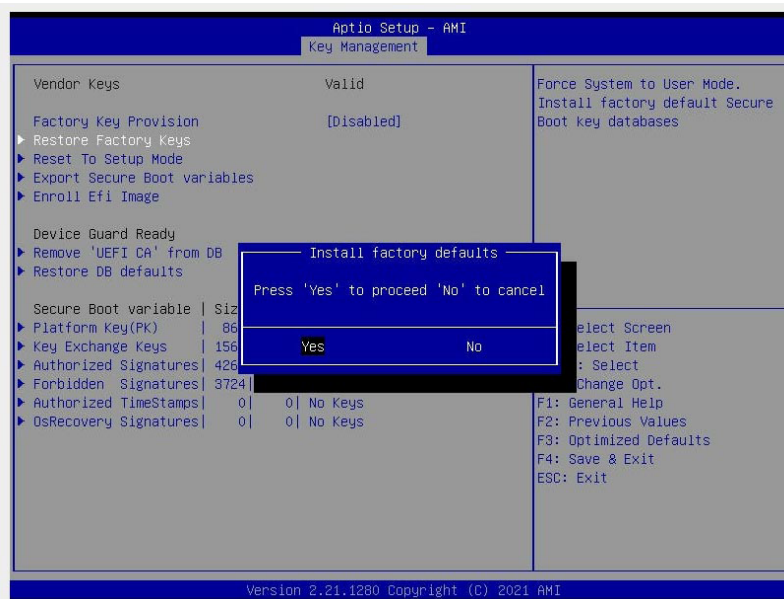
Factory Key Provision Defaults

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.



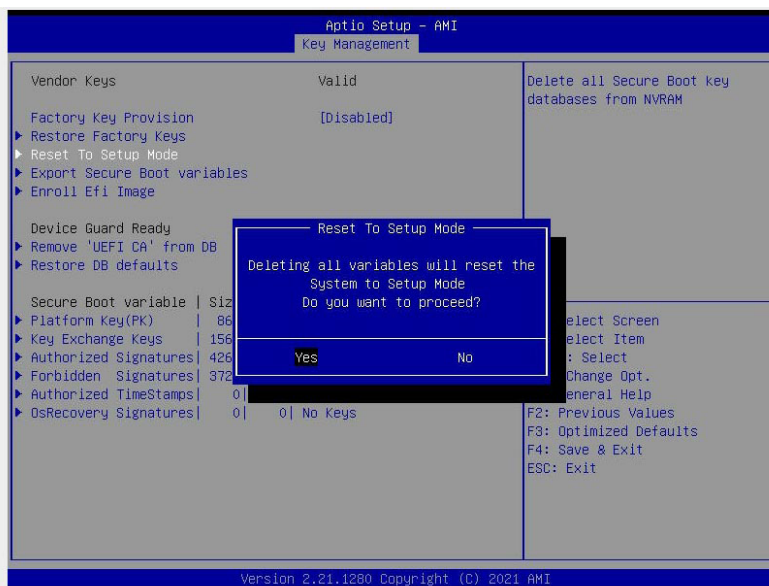
► Restore Factory Keys

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.



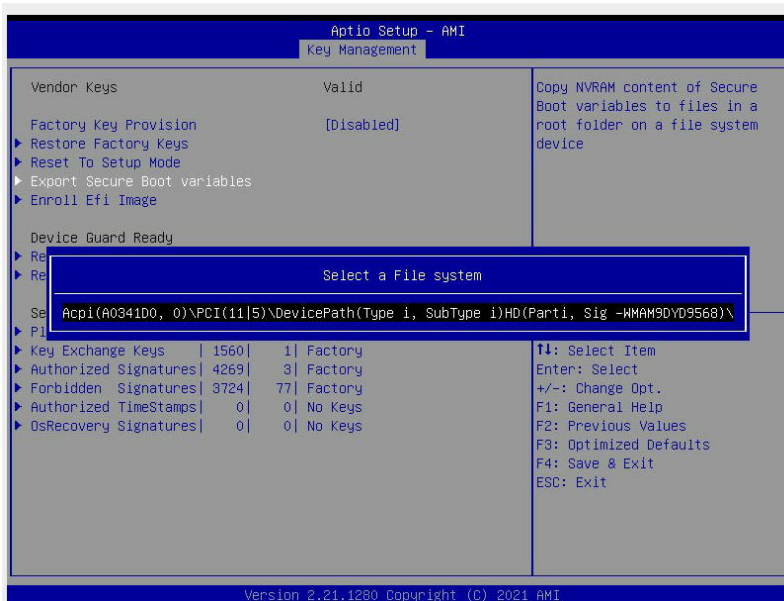
► Reset To Setup Mode (Available when the System Mode is in User mode)

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



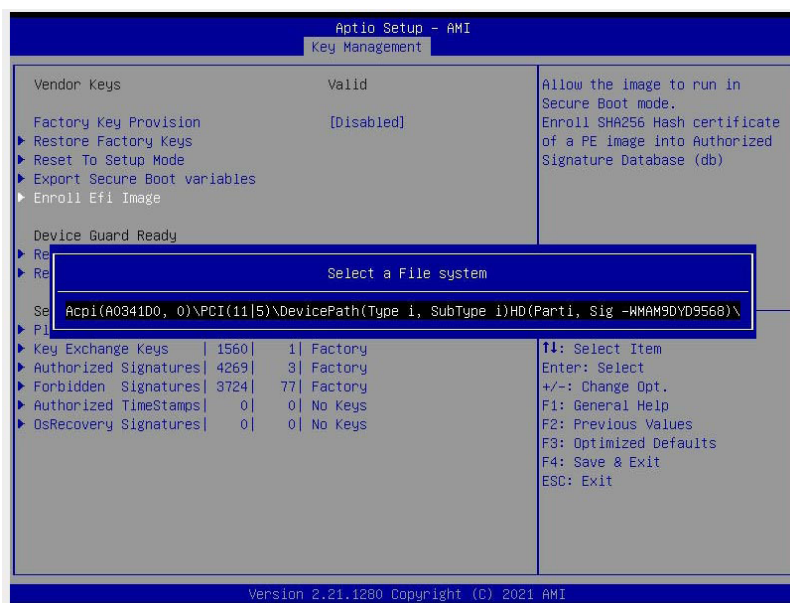
► Export Secure Boot Variables

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



► Enroll Efi Image

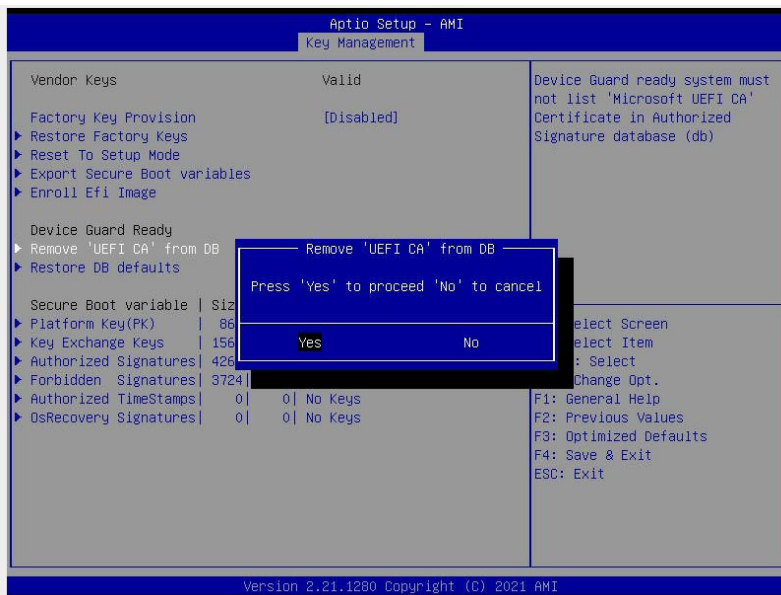
This feature enrolls SHA256 hash binary data in the Authorized Signature Database (DB) and allows the image to run in Secure Boot mode.



Device Guard Ready

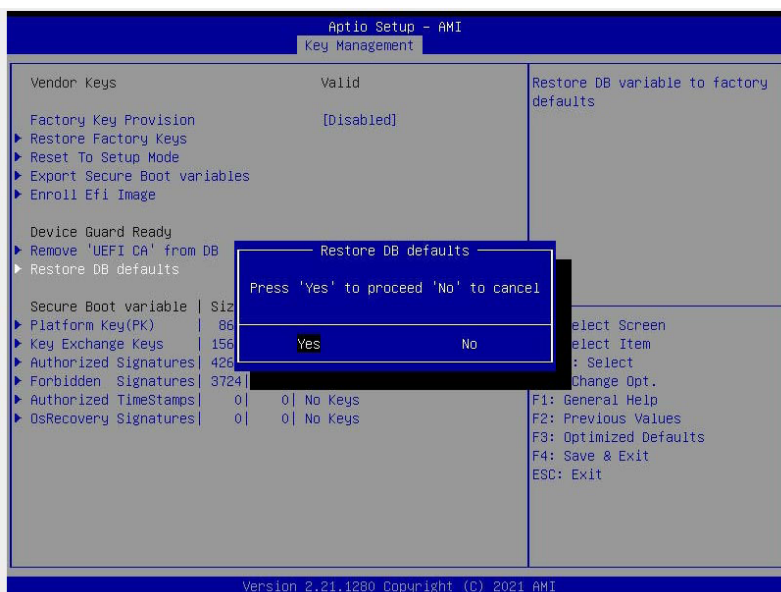
► Remove 'UEFI CA' from DB (Database) (available when the system is not in Device Guard Ready)

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



► Restore DB (Database) defaults

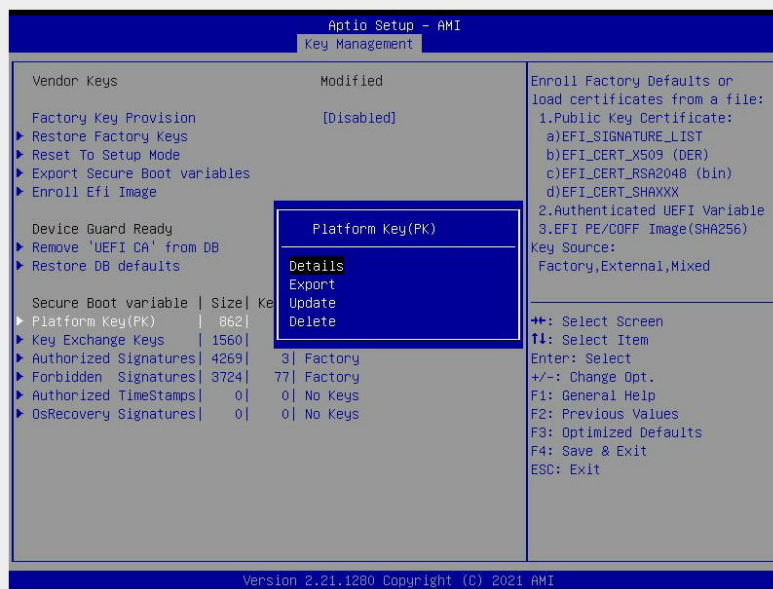
Select Yes and press <Enter> to restore the DB variables to the manufacturer default settings. The options are **Yes** and No.



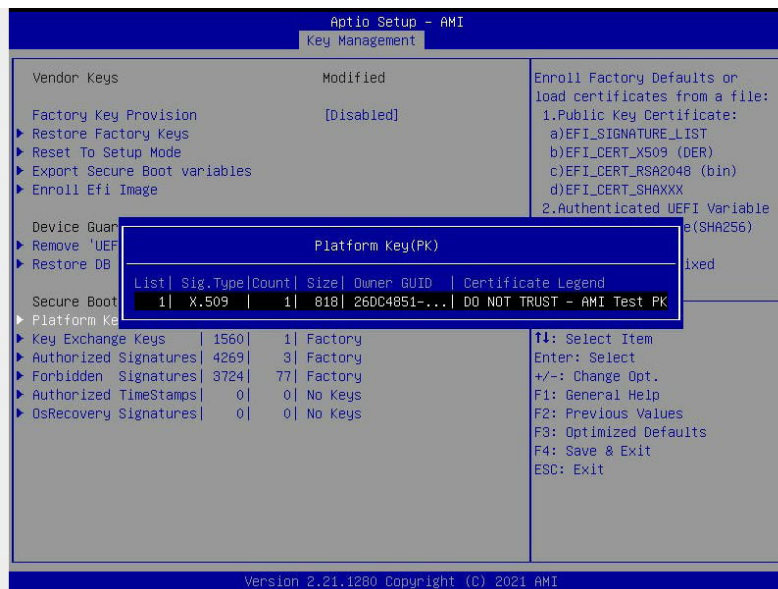
Important keys and signatures used in Secure Boot

► Platform Key (PK)

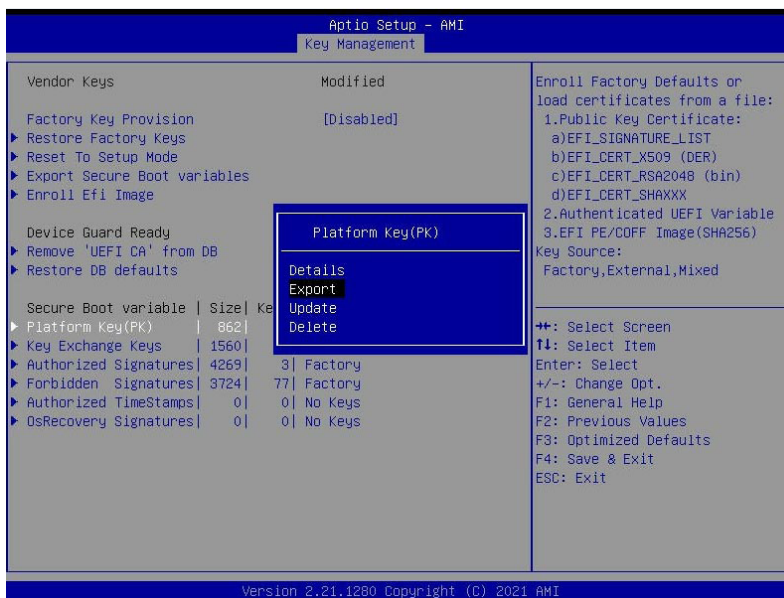
The Platform Key (PK), which is pre-installed in the system firmware during manufacturing, provides the full control of key hierarchy in Secure Boot. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to 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.



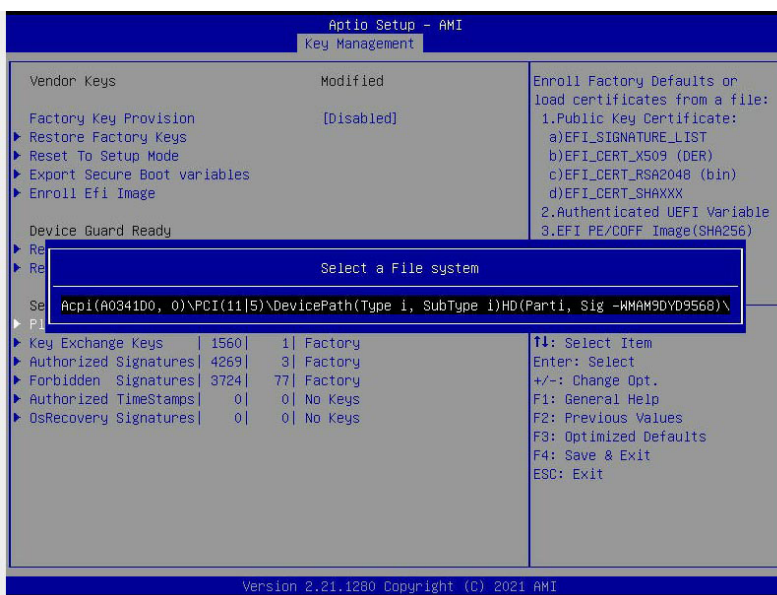
Details: Use the arrow keys to select **Details** (default) and press <Enter>. This displays detailed information of PK as shown below.




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

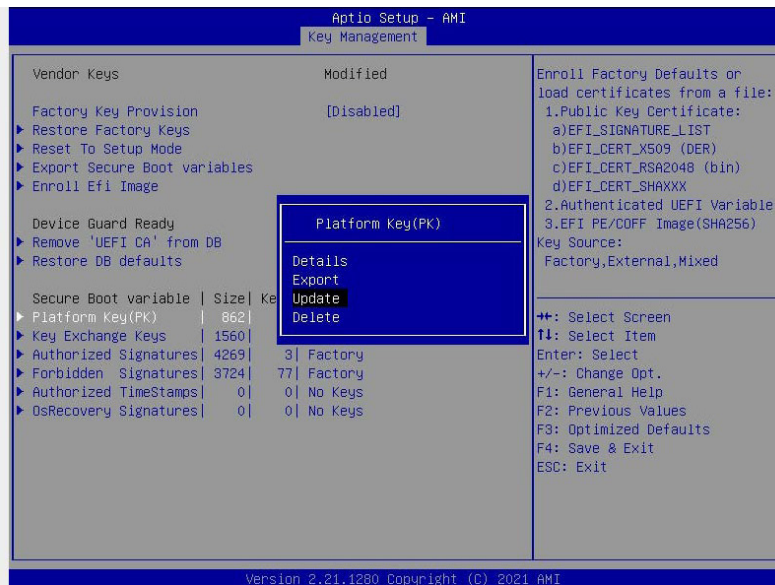


Press <Enter> and the following screen will appear.

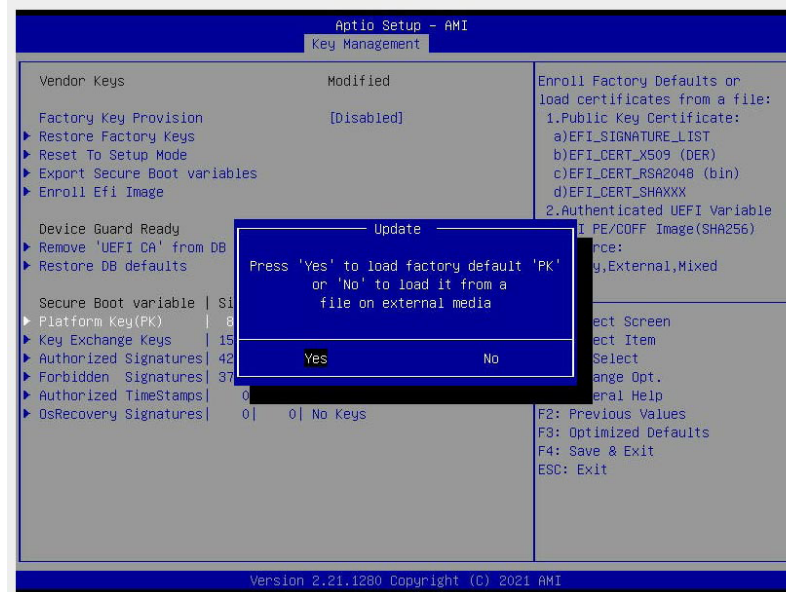


 **Note:** Refer to the right panel of the screen to display the file formats that are supported by your platform.

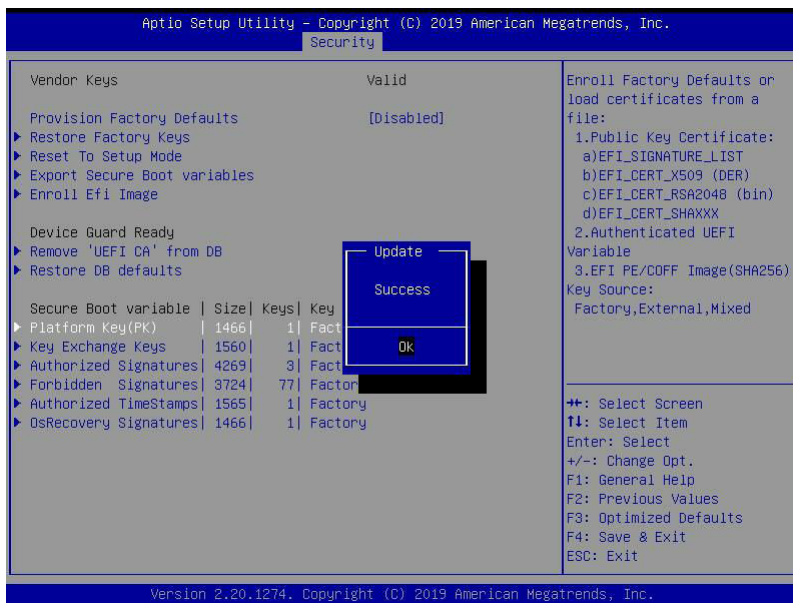
Update: Use the arrow keys to select Update. This will load the manufacturer defaults or load PKs from a file in an external device.



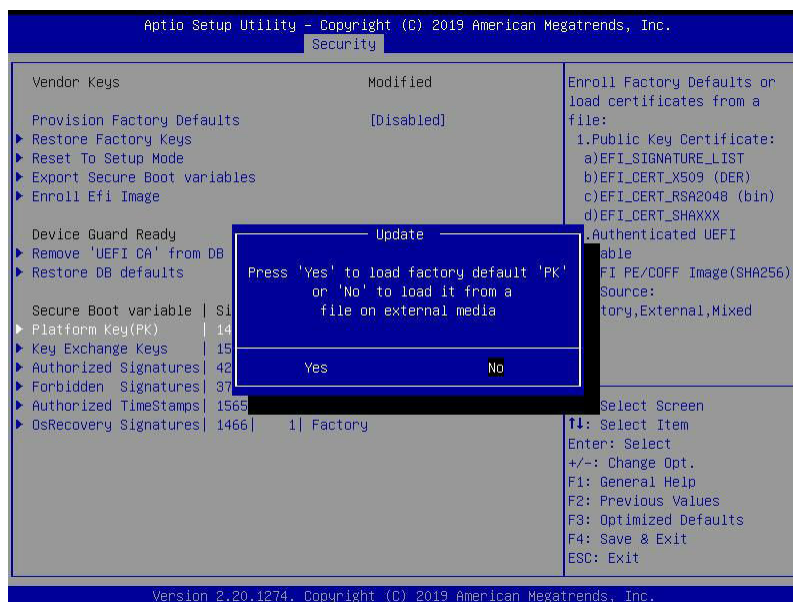
Press <Enter> and the following screen will appear.



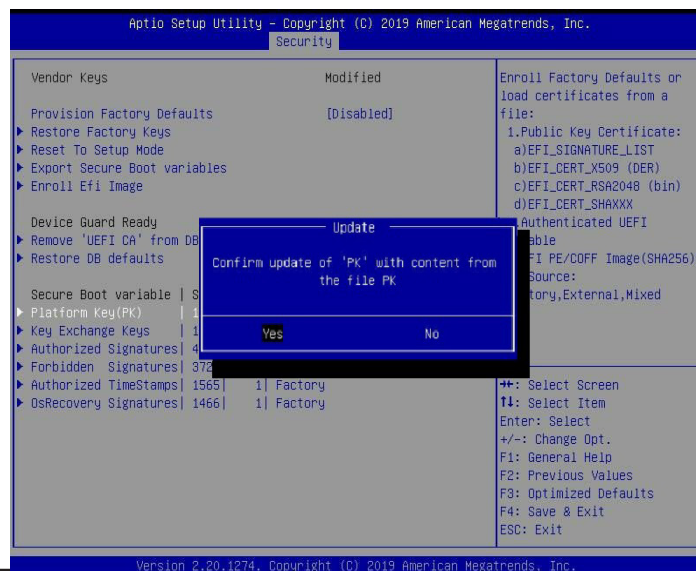
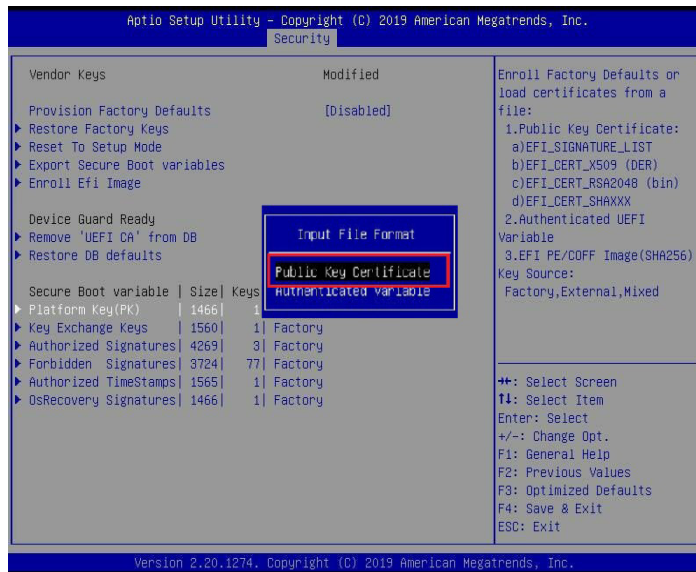
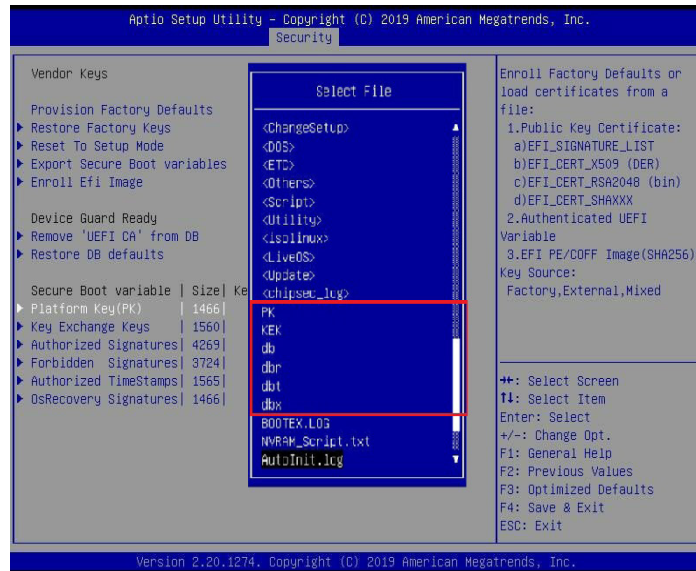
To load the manufacturer defaults, select Yes and press <Enter>. The following screen will appear.



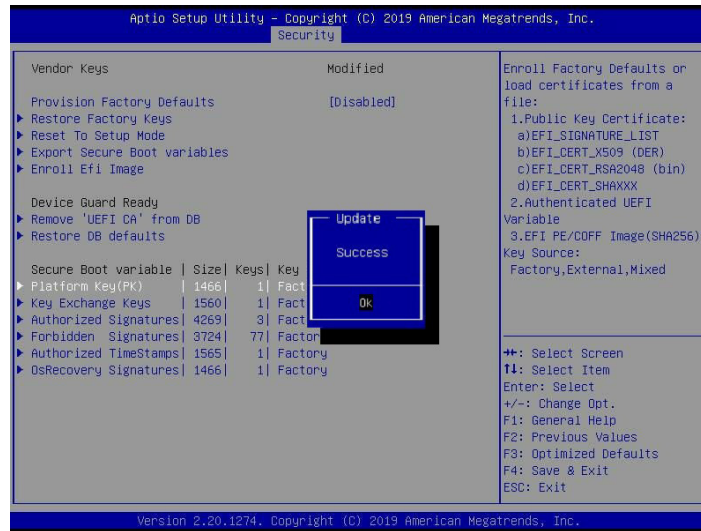
To load PKs from a file in an external device, select No and press <Enter>.



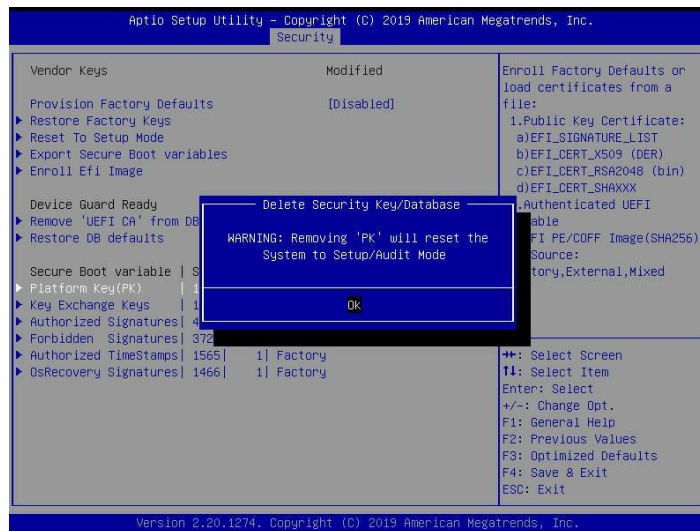
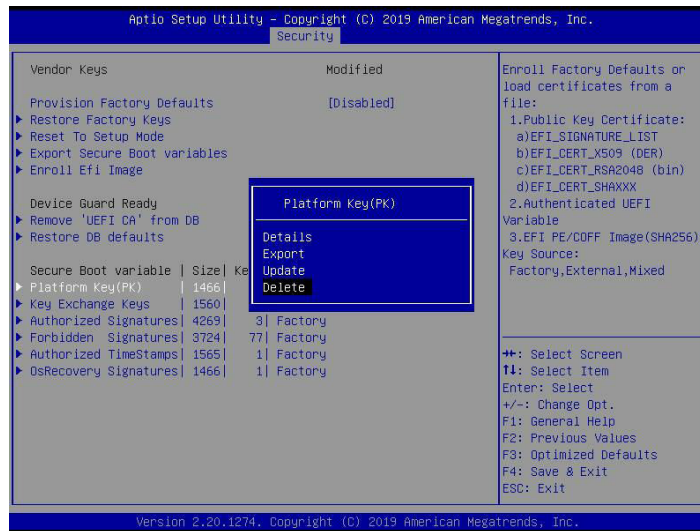
When the following screens appear, select the USB flash drive that contains the desired file and press <Enter>.



Press <Enter> and the following screen will appear.

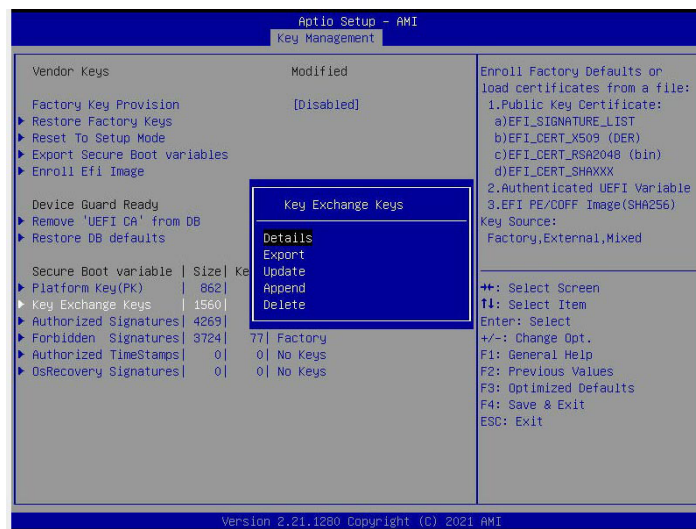


Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to Setup mode.

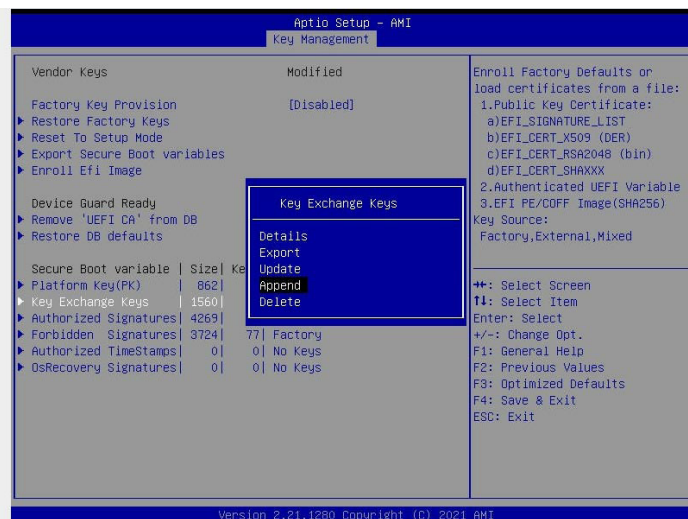


► Key Exchange Key

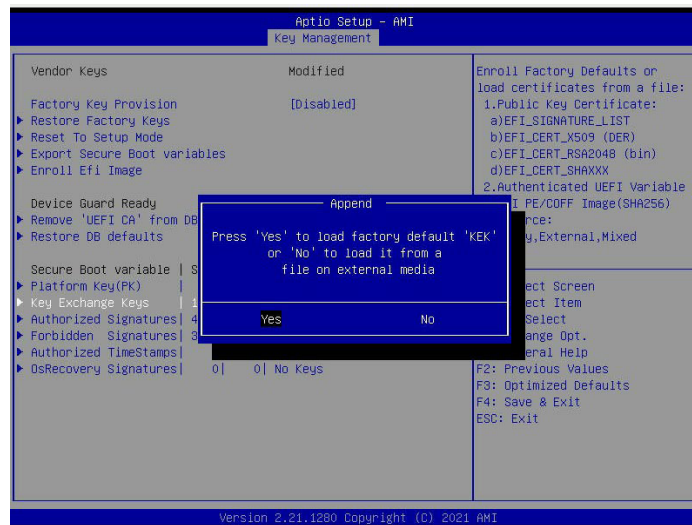
The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and is used in Secure Boot to protect the data base that contains signatures from being illegal accessed. The options are **Details**, Export, Update, Append, and Delete. Select Details to 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 Append 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.)



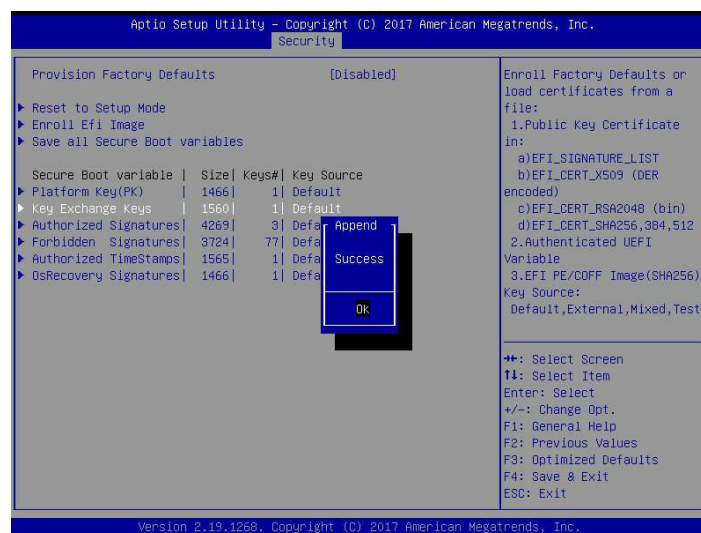
Append: Use the arrow keys to select Append.



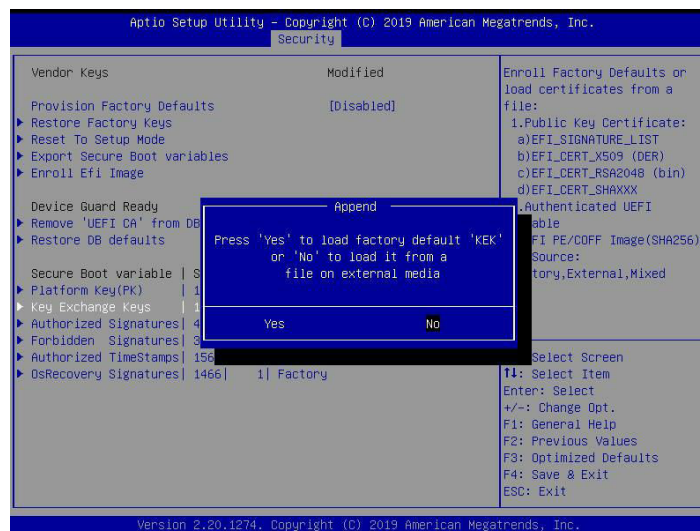
Press <Enter> and the following screen will appear.



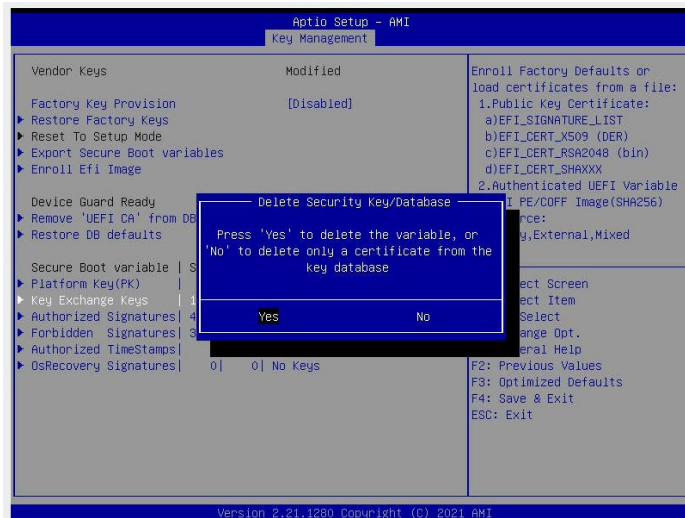
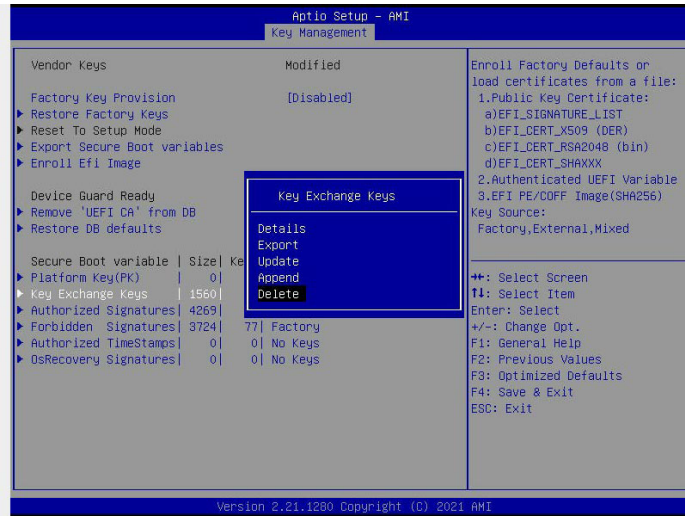
To load the manufacturer defaults, select Yes and press <Enter>. The following screen will appear.



To load 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.



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

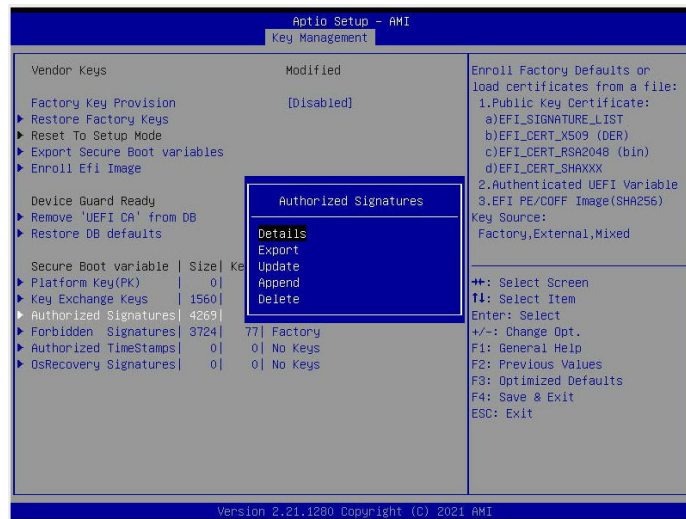


Select No and press <Enter> to delete only one certificate from the key database.



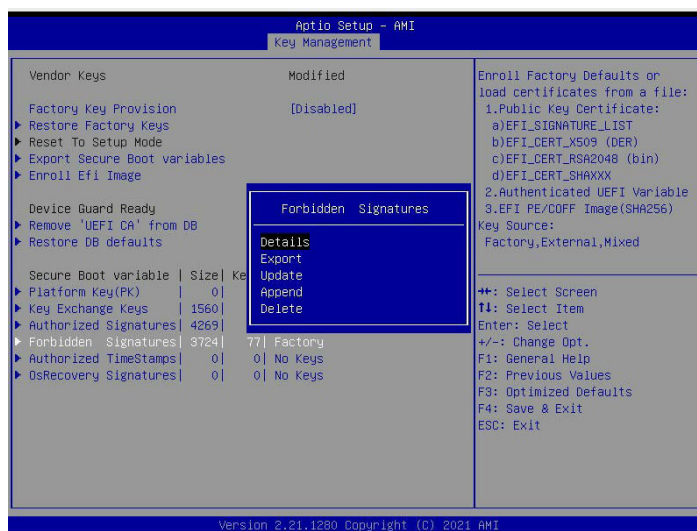
► Authorized Signatures

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.)



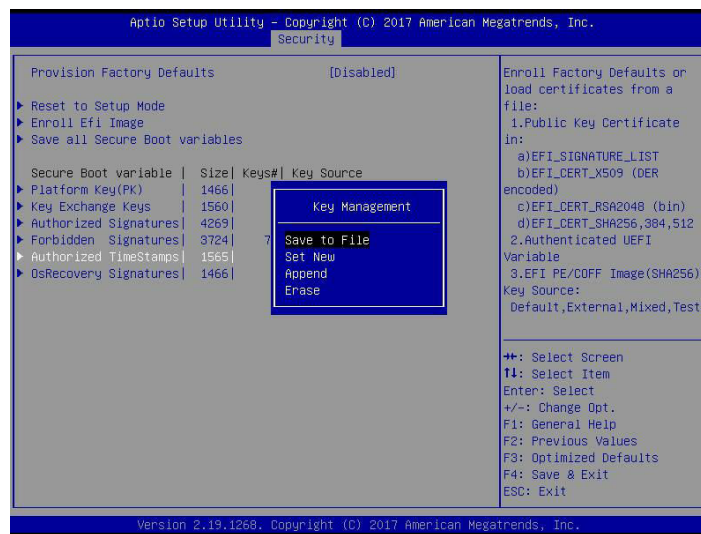
► Forbidden Signatures

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.)



► 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.)



► 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.)

