X12主板安全启动配置说明

用户指南

版本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 ultra-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

前言

关于本用户指南

本用户指南针对系统集成商、IT技术人员和有技术背景的最终用户编写。它介绍了如何在UEFI BIOS设置实用程序中为Supermicro的X12系列主板配置安全启动的相关信息。

本用户指南详细介绍如何在UEFI BIOS中为基于第三代Intel®Xeon®可扩展处理器的X12主板配置安全启动设置。请注意，Supermicro的所有产品只能由专业技术人员安装、配置和维修。

有关处理器/内存更新，请访问我们的网站http://www.supermicro.com/products/。

用户指南中使用的约定

应特别注意以下符号以正确配置BIOS，防止意外损坏系统组件：

备注：有关正确设置系统或正确配置固件的重要信息。

联系 Supermicro

总部

地址:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
电话:	+1 (408) 503-8000
传真:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
网站:	www.supermicro.com

欧洲

地址:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
电话:	+31 (0) 73-6400390
传真:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
网站:	www.supermicro.nl

亚太

地址:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
电话:	+886-(2) 8226-3990
传真:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
网站:	www.supermicro.com.tw

地址:	SUPERMICRO 科技（北京）有限公司 上海分公司 中国上海市漕溪北路398号702室
邮编:	200030
电话:	+86-021-61152556/7/8
Email:	Support-cn@supermicro.com（技术支持）
网站:	www.supermicro.org.cn

Table of Contents

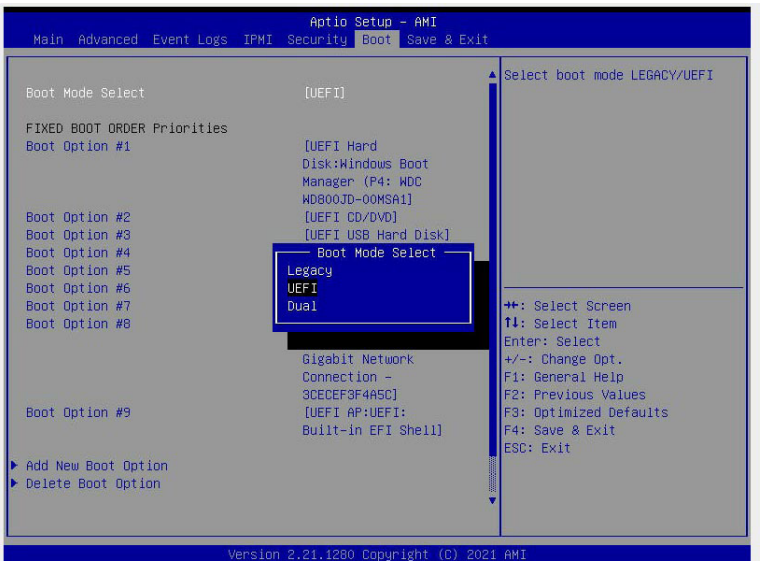
配置安全启动设置

安全启动是统一可扩展固件接口（UEFI）BIOS中的一项功能，通过防止驱动程序和操作系统加载程序在没有可接受数字签名情况下启动，从而实现安全启动。安全启动确保启动加载程序在系统启动时已取得数字签名和验证。使用机器前，必须正确配置安全启动设置。本文档第1~3节介绍如何在UEFI中启用安全启动功能。第4节介绍如何配置Key Management设置。要配置BIOS设置实现安全启动，请按照以下说明操作。

第1节 将启动模式设置为UEFI

由于安全启动是UEFI的一项功能，您需要按照以下步骤先在UEFI中启用安全启动模式。

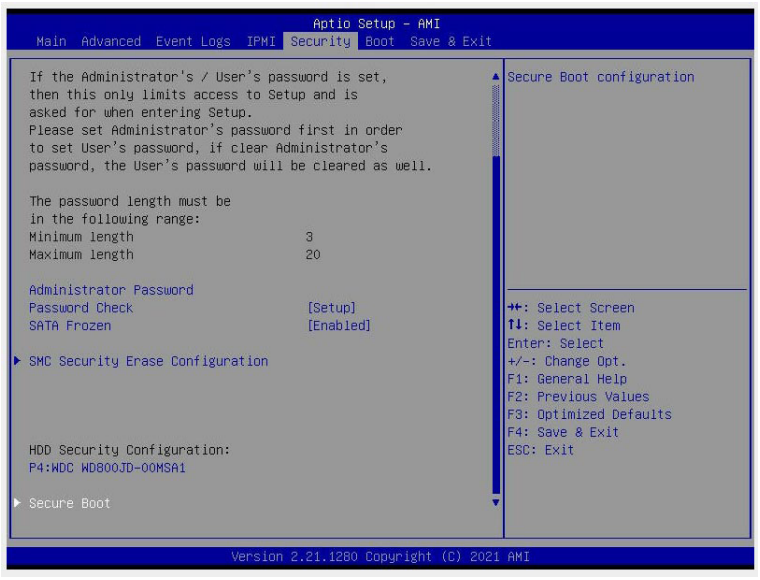
1. 系统启动时按<Del>，进入BIOS设置实用程序。
2. 从屏幕顶部菜单栏中选择Boot（启动）选项卡，然后按<Enter>。使用向下箭头键向下滚动以选择功能：Boot Mode Select并按<Enter>。
3. Boot Mode Select设置选项（包括LEGACY、UEFI和DUAL）将显示如下。从启动选项中选择UEFI并按<Enter>将启动模式设置为UEFI。
4. 要使更改生效，请按<F4>保存设置并重新启动系统。



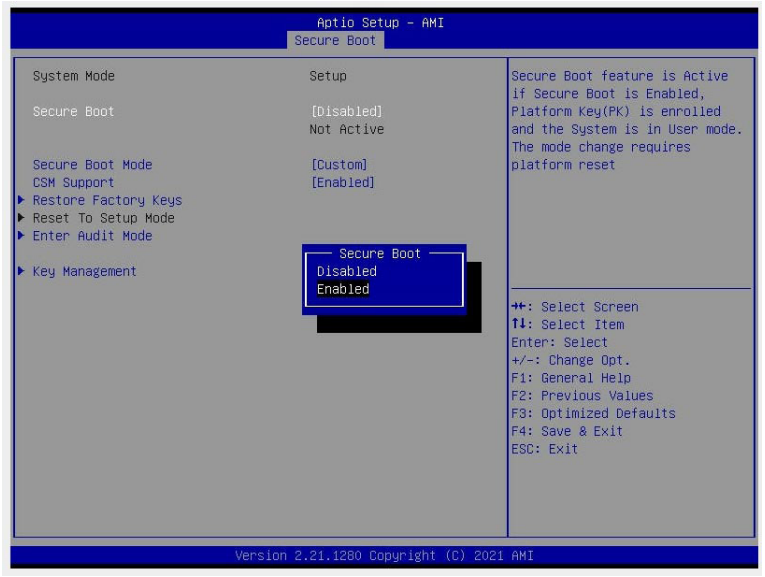
第2节 安全启动/安全启动模式/CSM支持

要使用安全启动功能，您需要在系统所运行的平台上预先注册一组平台密钥（PK）。还需要启用安全启动功能，将安全启动模式设置为自定义，并在BIOS设置实用程序中禁用CSM支持。请按照以下说明进行操作：

系统启动时按<Del>，进入BIOS设置。从顶部菜单栏选择Security。



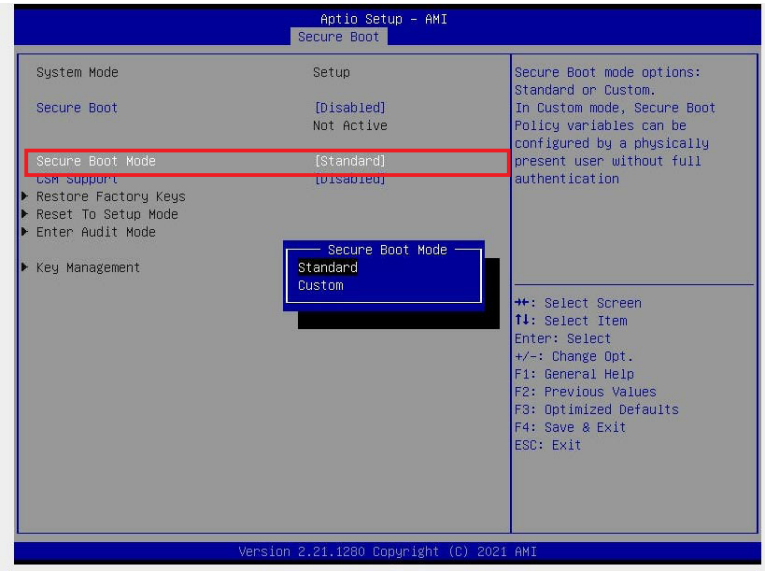
上面屏幕显示时，选择Secure Boot（安全启动）并按<Enter>访问菜单项。以下屏幕将显示。



第3节 安全启动设置

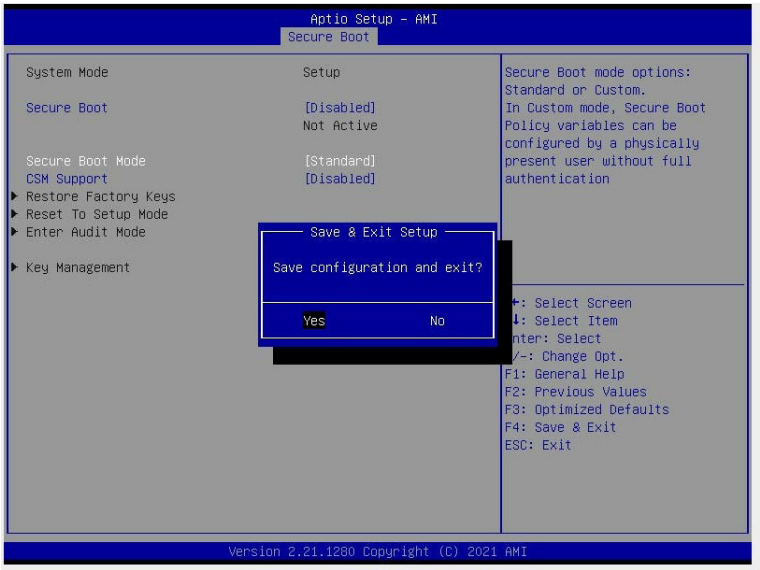
要正确配置安全启动设置，请执行以下步骤。

步骤1. 将安全启动模式设置为Standard（标准）。按Yes（是）根据需要安装制造商默认密钥。

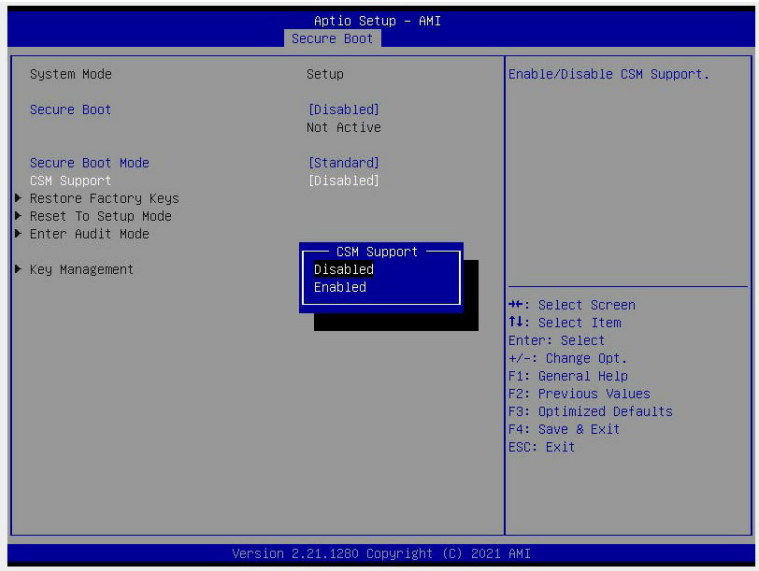


备注：当安全启动模式设置为标准时，Key Management（密钥管理）菜单将不可用。

步骤2. 要使更改生效，请按<F4>保存设置并退出BIOS设置实用程序。

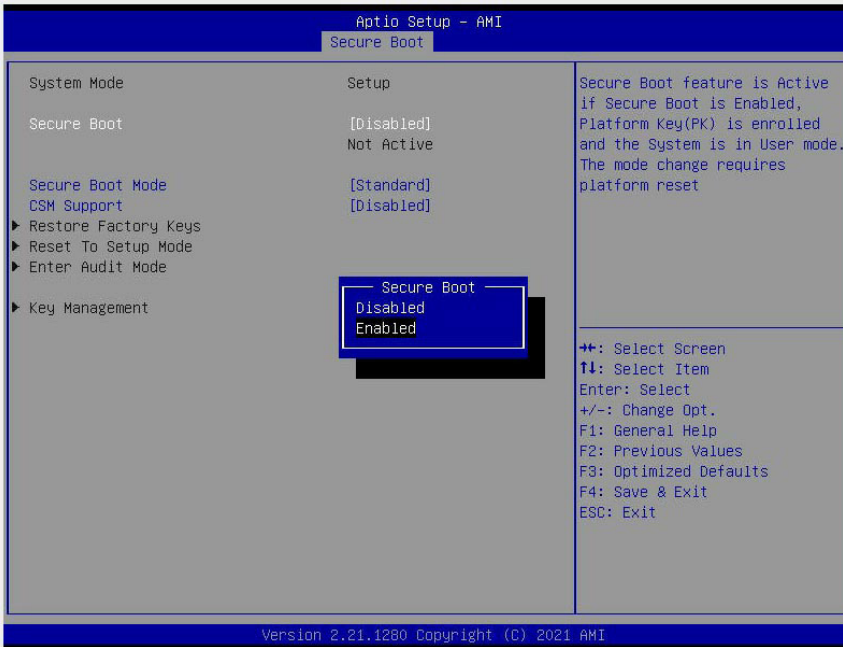


步骤3. 系统启动时按<Del>，进入BIOS设置实用程序。导航至Security（安全）选项卡以进入安全启动菜单。如第1节所述，将CSM支持设置为Disabled（禁用）。

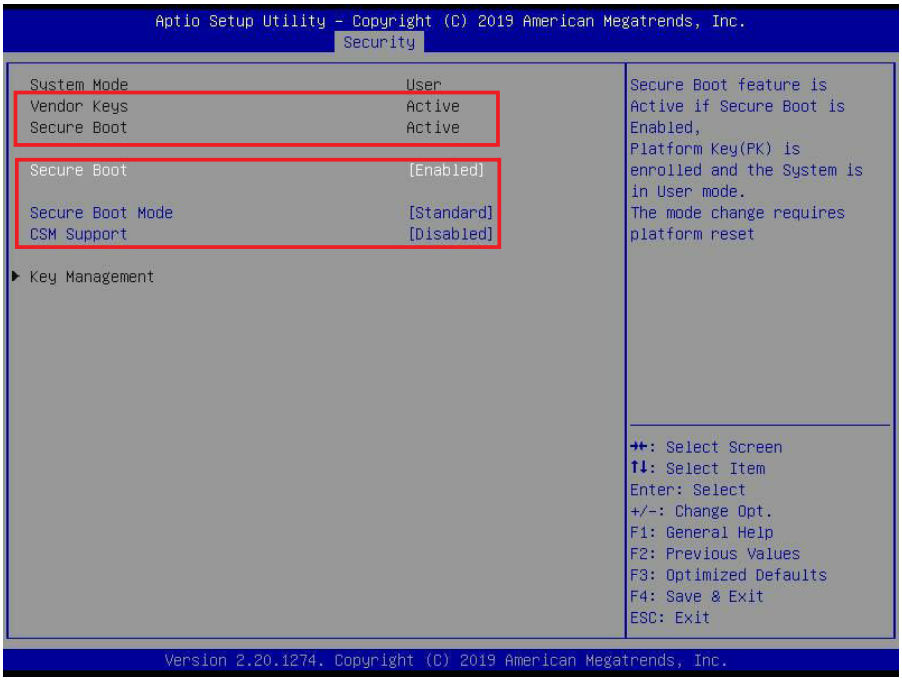


要使更改生效，请按<F4>保存设置并退出BIOS设置实用程序。

步骤4. 系统启动时按<Del>，进入BIOS设置实用程序。导航至Security（安全）选项卡并进入安全启动菜单。将安全启动设置为Enabled（启用）。



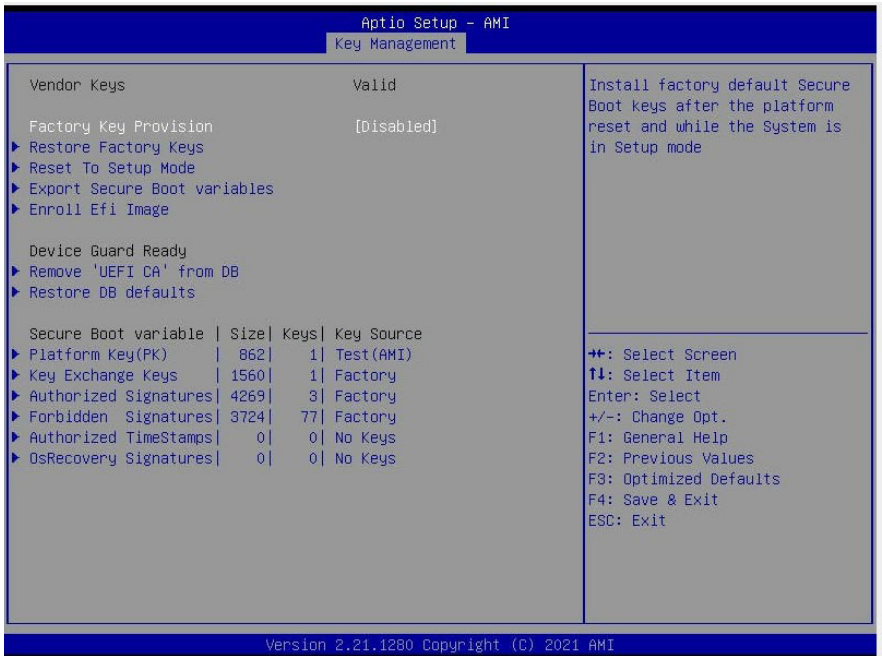
要使更改生效，请按<F4>保存设置并退出BIOS设置实用程序。系统启动时按<Del>，进入BIOS设置实用程序。导航至Security（安全）选项卡并进入安全启动菜单。以下屏幕将显示。



备注：启用安全启动后，CSM支持将被禁用，传统平台将不再受支持；平台中只允许已授权UEFI应用程序，如UEFI OS、AOC UEFI FW和UEFI PXE服务器。

第4节 Key Management设置

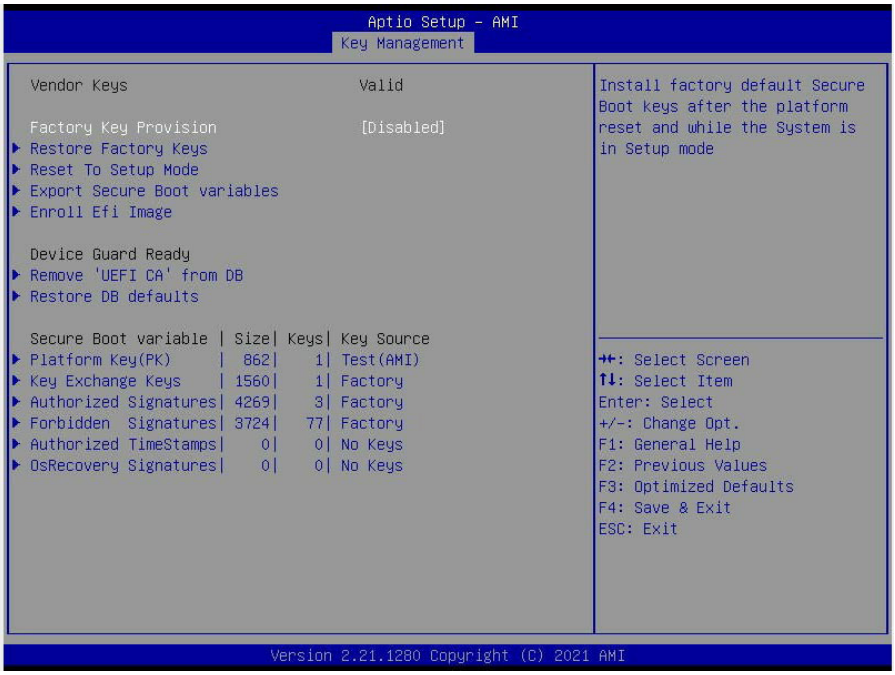
Key Management（密钥管理）菜单（仅当安全启动模式设置为自定义时可用）允许通过外部设备安装安全启动密钥并用于安全系统启动。



Vendor Keys（供应商密钥）

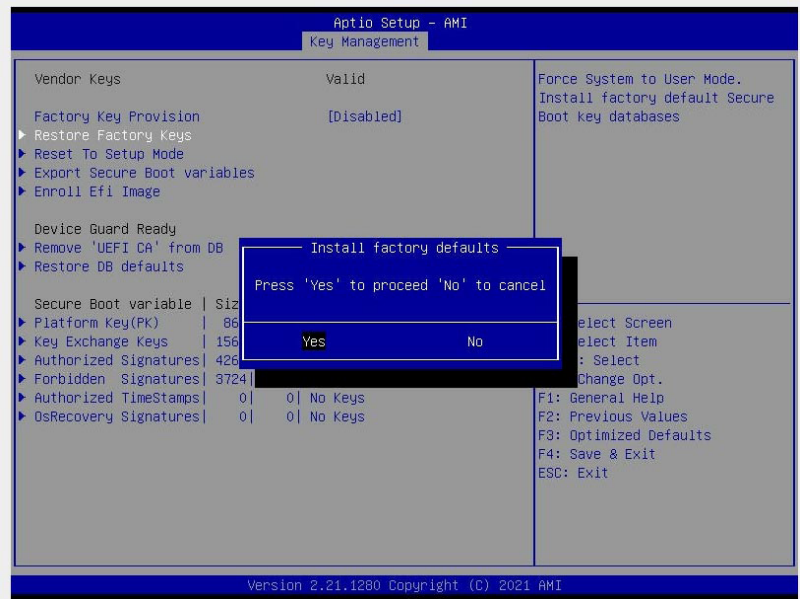
Factory Key Provision Defaults（工厂密钥预配默认值）

当系统处于设置模式时，此功能用于预配制造商预先设置的默认安全启动密钥。选择**Disabled（禁用）**以使用自己的安全启动密钥启动系统。



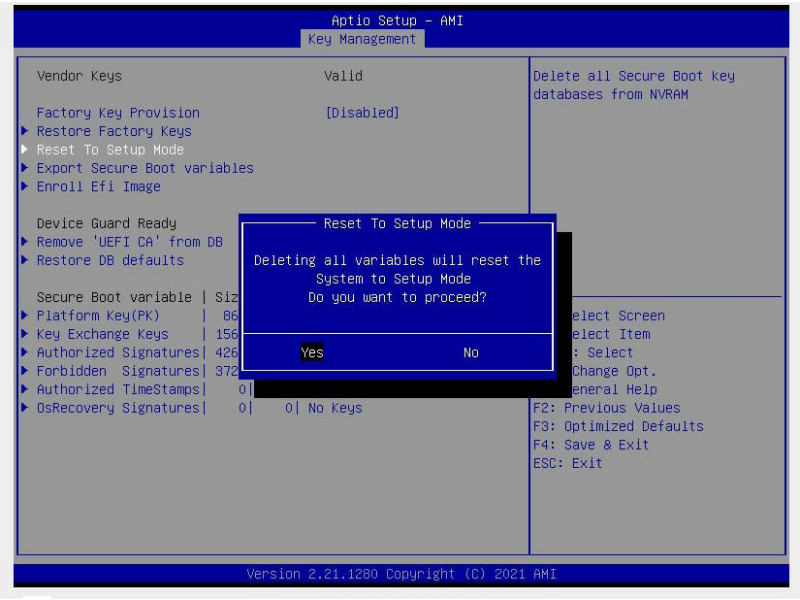
▶ Restore Factory Keys（恢复工厂密钥）

选择Yes（是），然后按<Enter>恢复制造商默认安全启动密钥。这也会将系统重置为用户模式。选项为 **Yes（是）**和 No（否）。



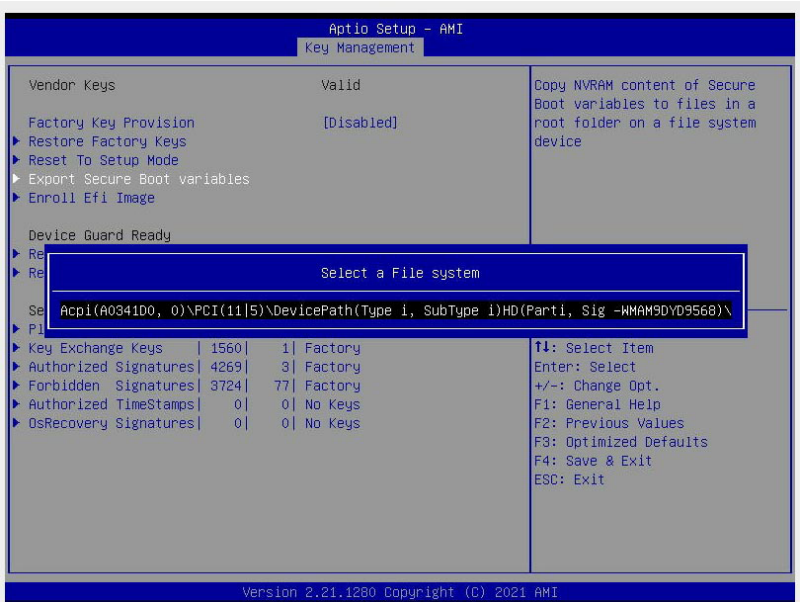
▶ Reset To Setup Mode（重置为设置模式）（系统处于用户模式时可用）

选择Yes（是），然后按<Enter>清除所有安全启动值，并将系统重置为设置模式。选项为 **Yes（是）**和 No（否）。



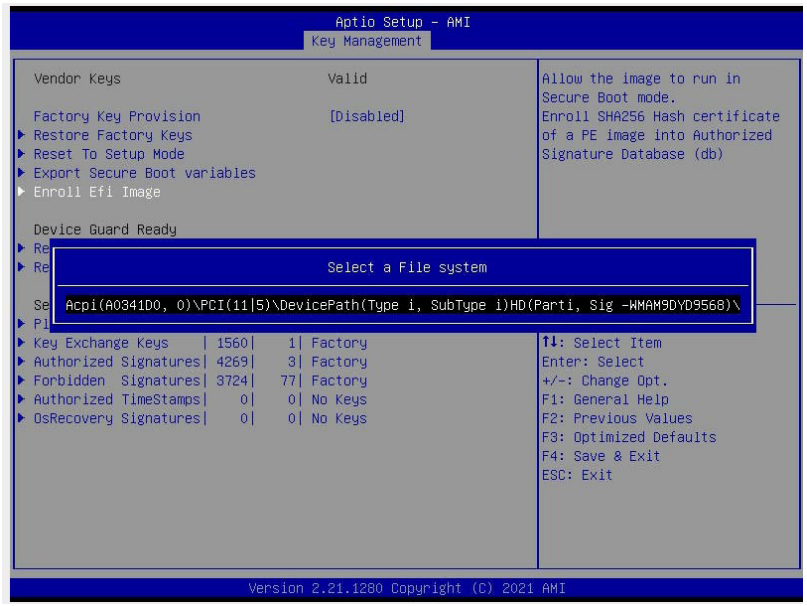
▶ Export Secure Boot Variables（导出安全启动变量）

使用此功能可将安全启动值导出至文件系统设备中根文件夹内的文件。



▶Enroll Efi Image（登记Efi镜像）

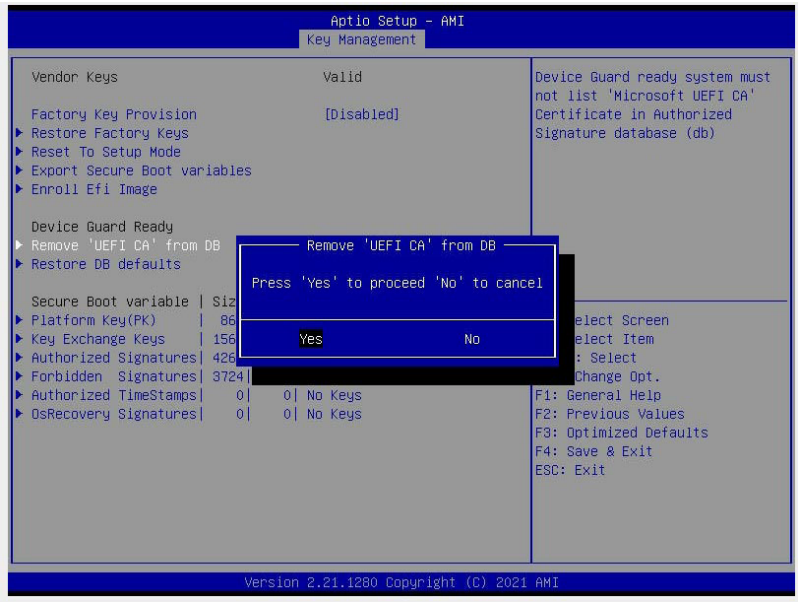
此功能在授权签名数据库（DB）中登记SHA256哈希二值数据，并允许镜像在安全启动模式下运行。



Device Guard Ready（设备卫士就绪）

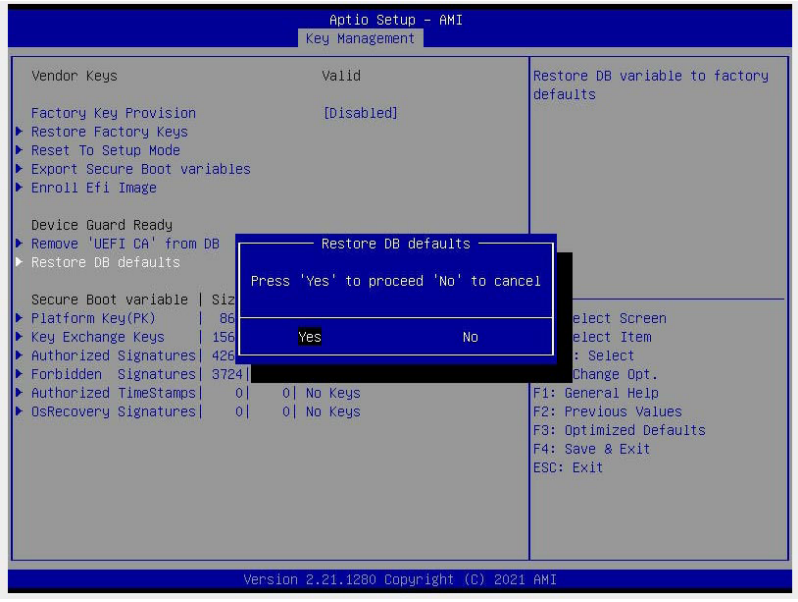
▶从DB（数据库）中删除“UEFI CA”（当系统未处于设备卫士就绪状态时可用）

选择Yes（是），然后按<Enter>从数据库（DB）中删除Microsoft UEFI CA证书。选项为 **Yes（是）** 和 No（否）。



▶ Restore DB (Database) defaults（恢复数据库默认值）

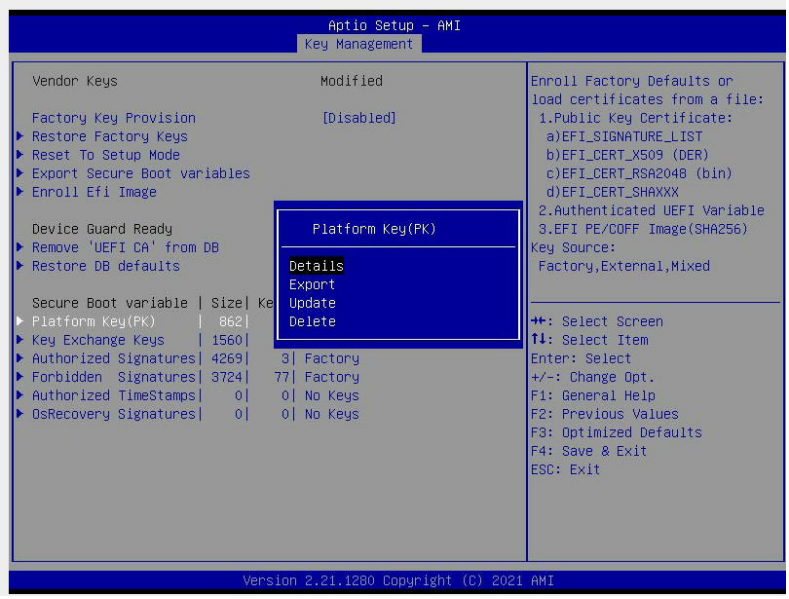
选择Yes（是），然后按<Enter>将数据库变量恢复为出厂默认设置。选项为 **Yes（是）** 和 No（否）。



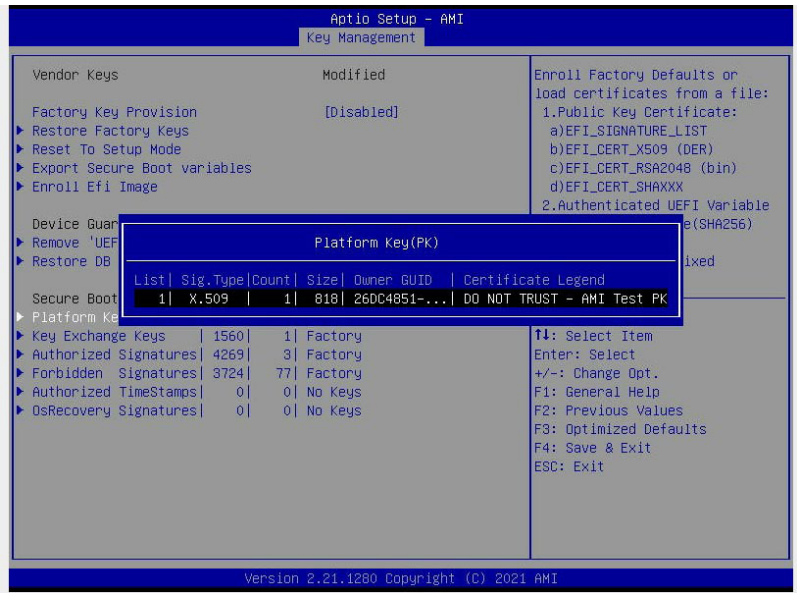
安全启动中使用的重要密钥和签名

▶平台密匙（PK)

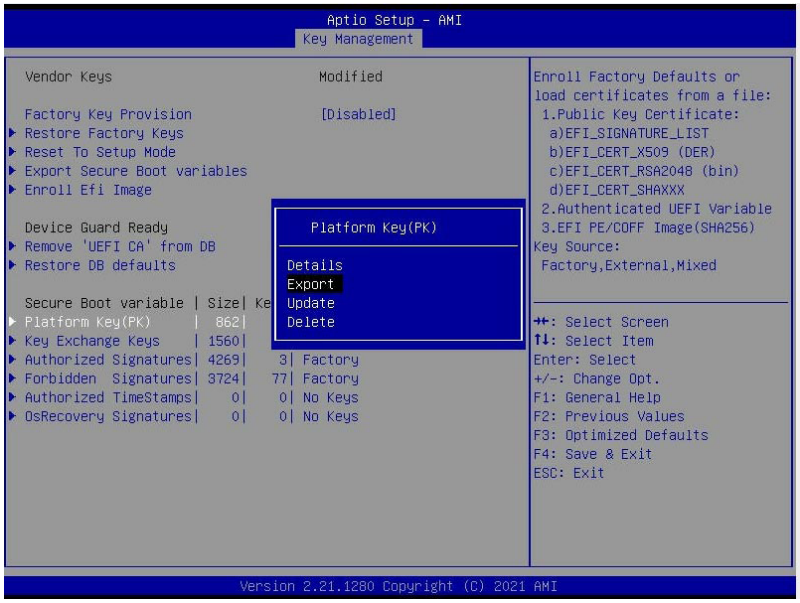
平台密钥(PK)在制造过程中预安装在系统固件中，可完全控制安全启动中的密钥层次结构。选项包括**详细信息**、导出、更新和删除。选择Details（详细信息）显示PK的详细信息。选择Export（导出）将当前PK保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载PK。选择Delete（删除）清除当前PK并将系统重置为设置模式。有关更多信息，参见以下屏幕。



Details（详细信息）：使用箭头键选择**详细信息**（默认），然后按<Enter>。这将显示PK的详细信息，如下所示。



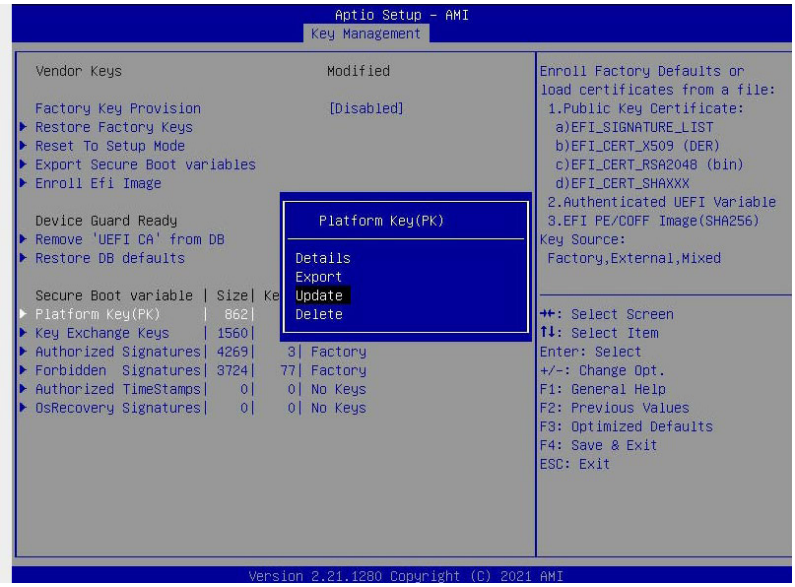
Export（导出）：使用箭头键选择“导出”并按<Enter>。此选项将当前PK保存到FAT格式的U盘。



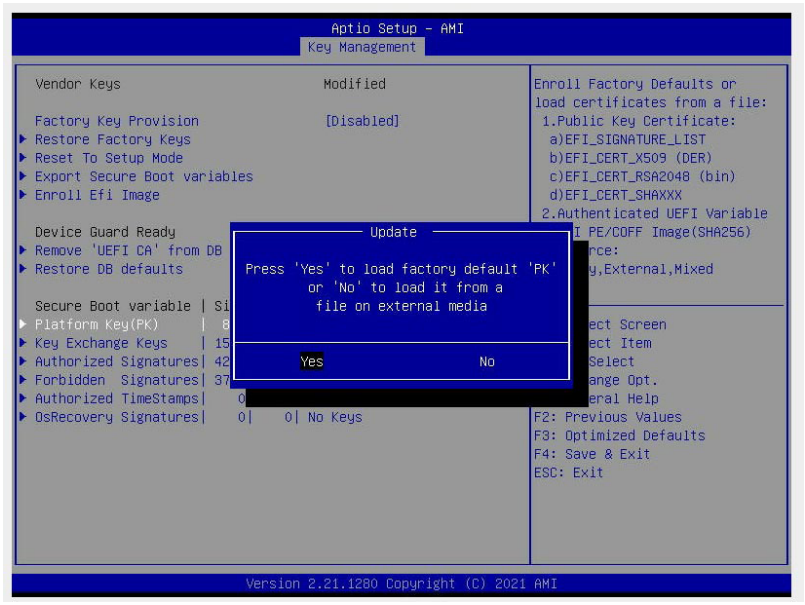
按<Enter>，以下屏幕将显示。

备注：参见屏幕右面板以显示平台支持的文件格式。

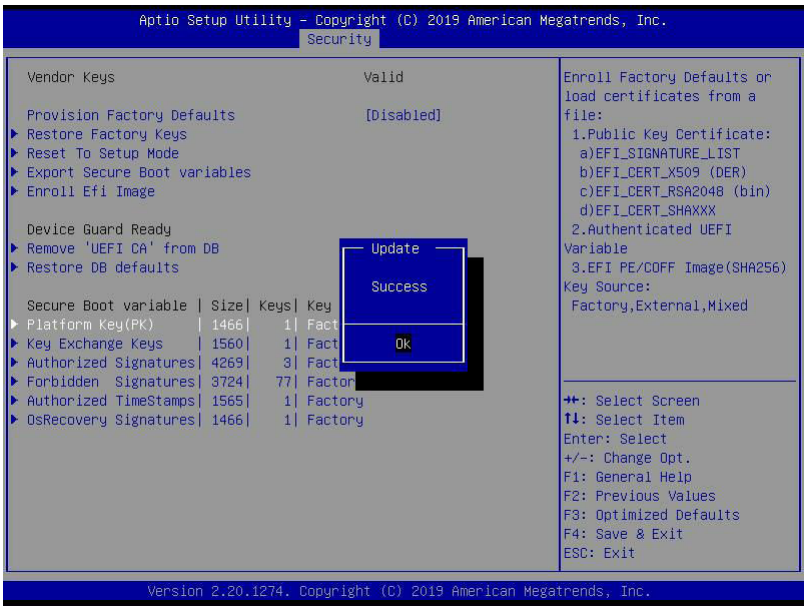
Update（更新）： 使用箭头键选择“更新”。这将加载制造商默认值或从外部设备的文件中加载PK。



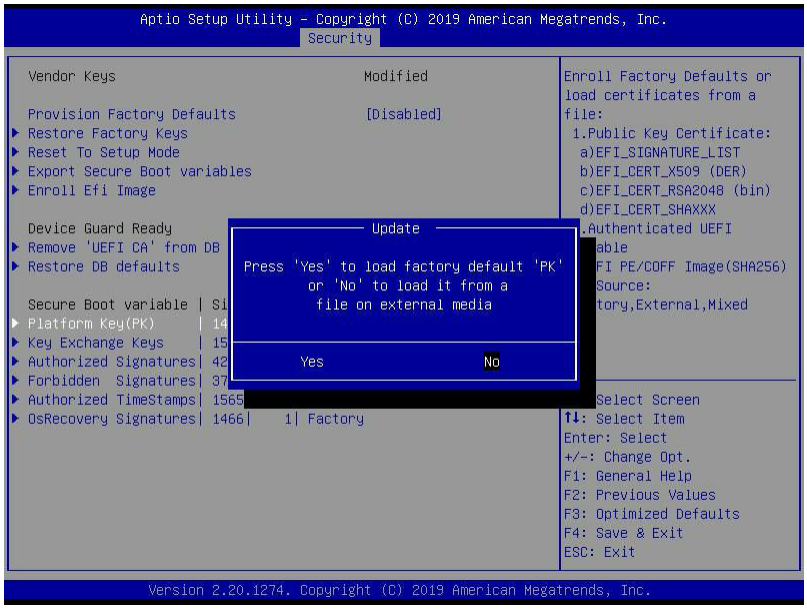
按<Enter>，以下屏幕将显示。



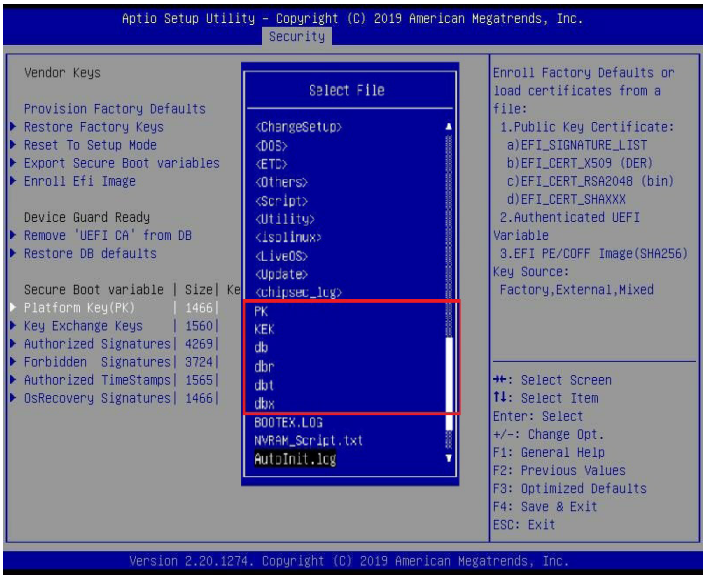
要加载制造商默认值，请选择Yes（是），然后按<Enter>。以下屏幕将显示。

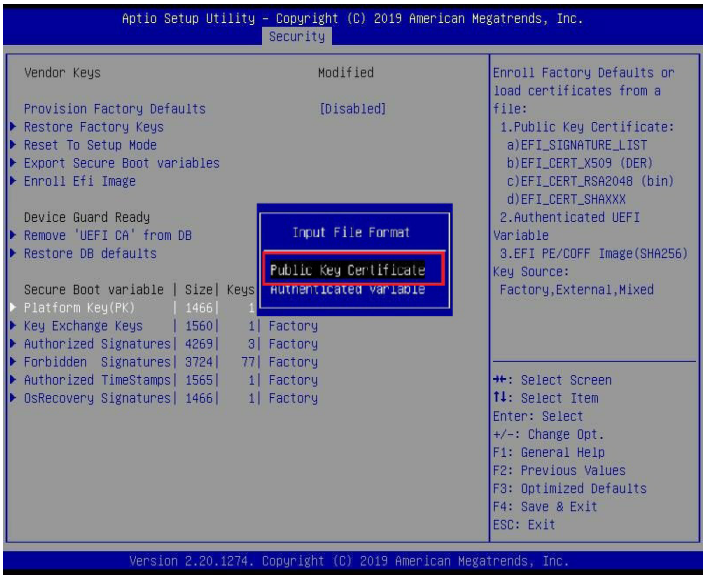


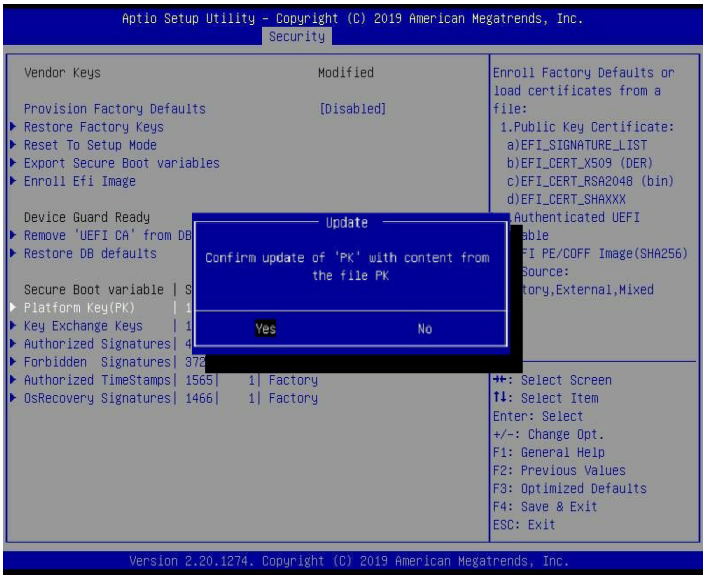
要从外部设备的文件中加载PK，请选择No（否），然后按<Enter>。



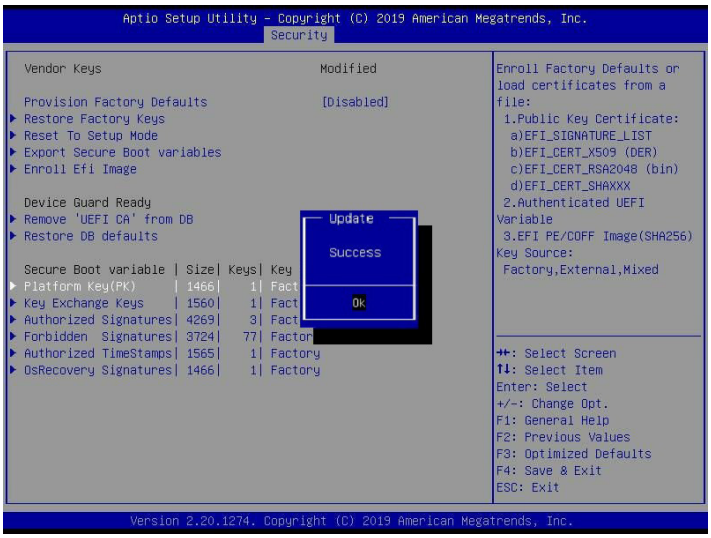
以下屏幕显示时，选择包含所需文件的U盘，然后按<Enter>。



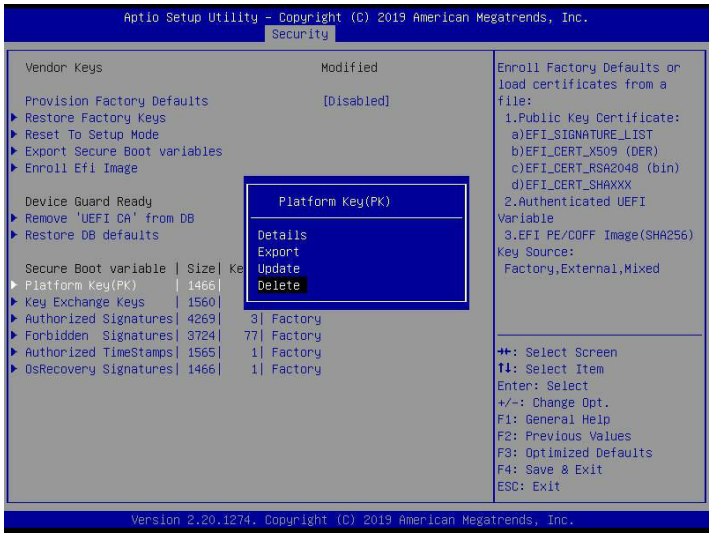


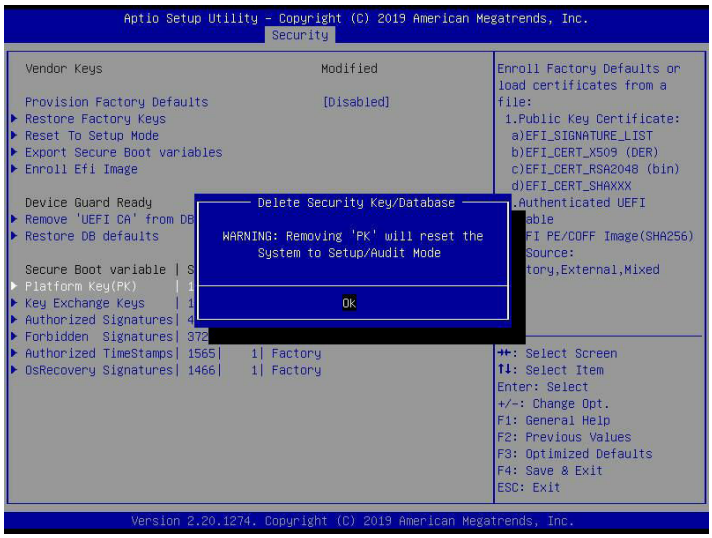


按<Enter>，以下屏幕将显示。



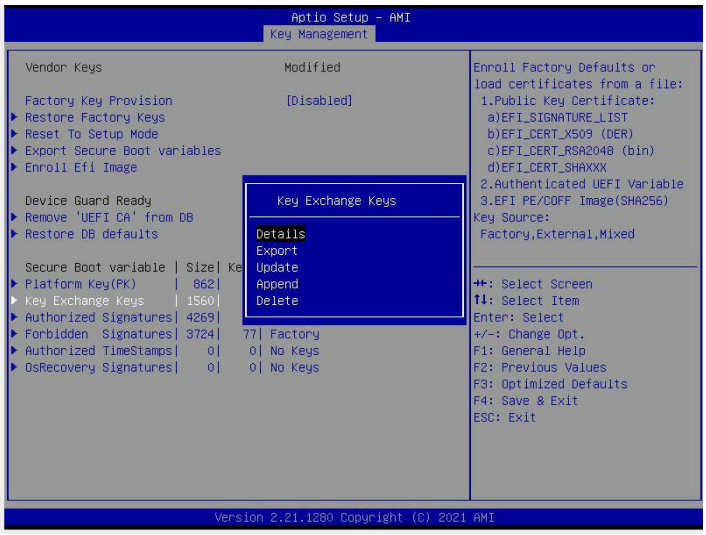
Delete（删除）：使用箭头键选择“删除”，然后按<Enter>清除当前PK并将系统重置为设置模式。



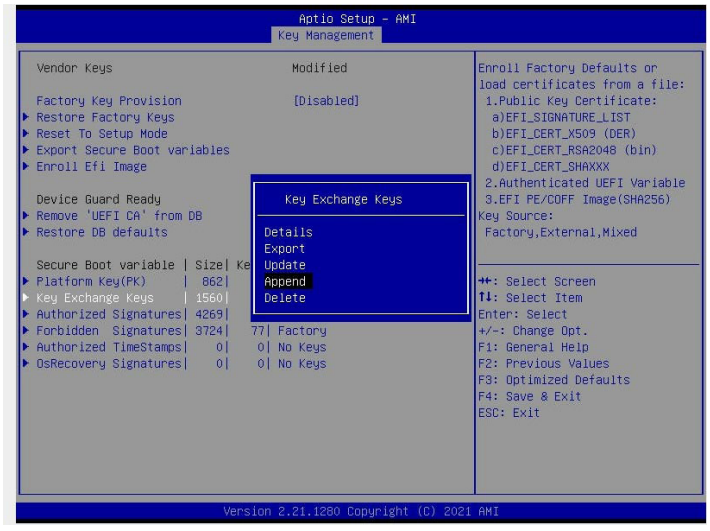


▶ Key Exchange Key（密钥交换密钥）

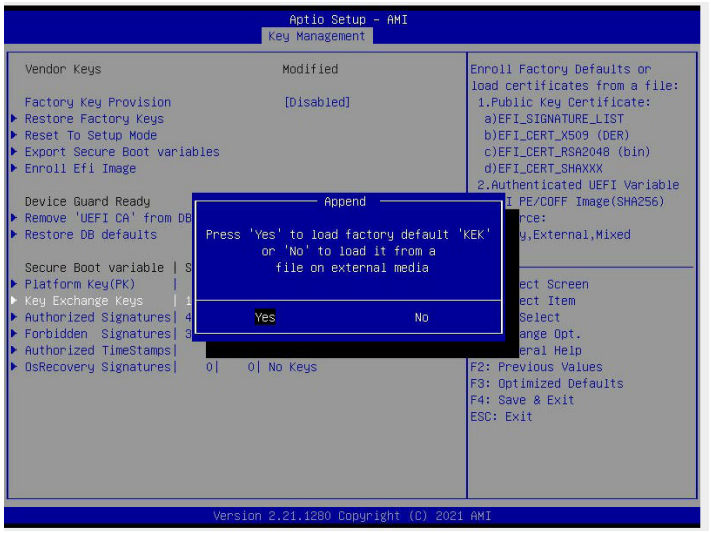
PK持有人可以更新操作系统供应商持有的密钥交换密钥（KEK），并用于安全启动，以保护包含签名的数据库免受非法访问。选项有**详细信息**、导出、更新、追加和删除。选择Details（详细信息）显示KEK的详细信息。选择Export（导出）将当前KEK保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载KEK。选择Append（追加）加载制造商默认值，或从外部设备的文件中加载KEK。选择Delete（删除）清除当前KEK或仅从密钥数据库中删除一个证书。（有关导出过程，参见第16页。有关更新过程，参见第17、18、19和20页。）



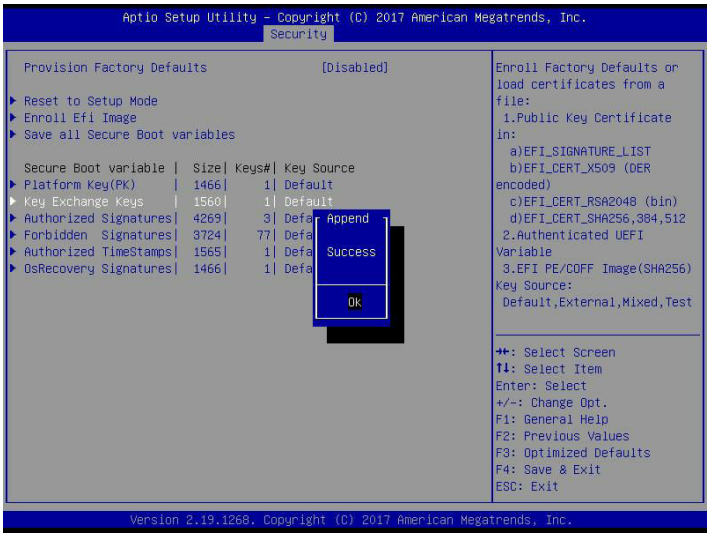
Append（追加）：使用箭头键选择“追加”。



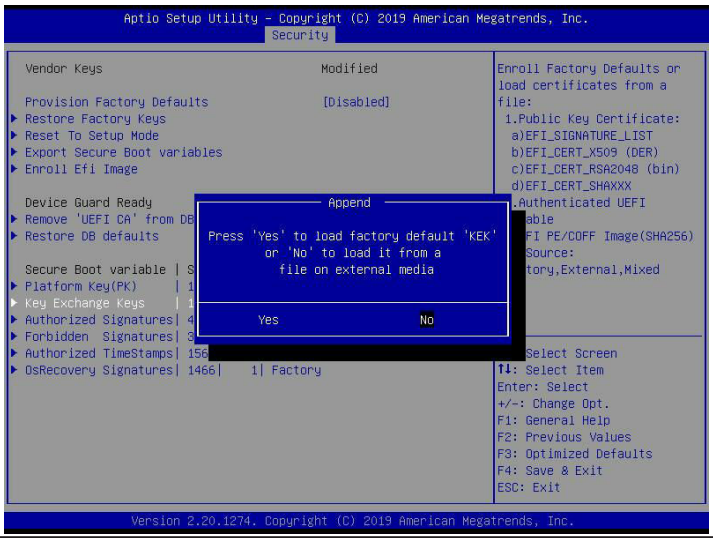
按<Enter>，以下屏幕将显示。



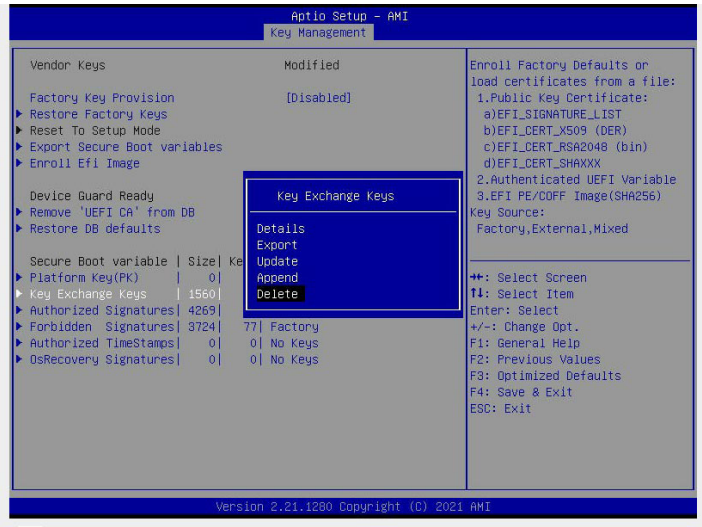
要加载制造商默认值，请选择Yes（是），然后按<Enter>。以下屏幕将显示。

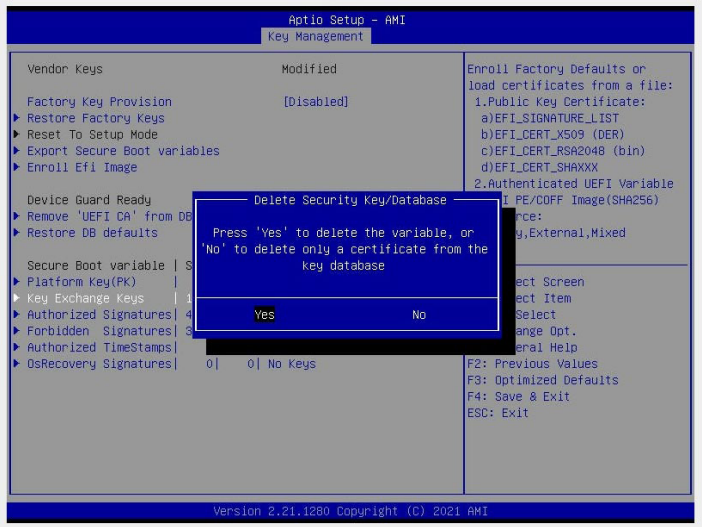


要从外部设备的文件中加载KEK，请选择No（否），然后按<Enter>。要了解如何从外部设备的文件中加载KEK，参见第21和22页。

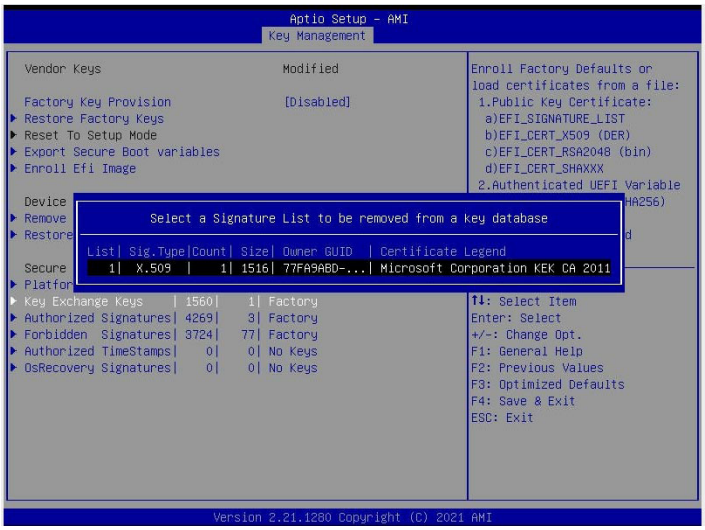


Delete（删除）：使用箭头键选择“删除”，然后按<Enter>。选择Yes（是），然后按<Enter>清除当前KEK。



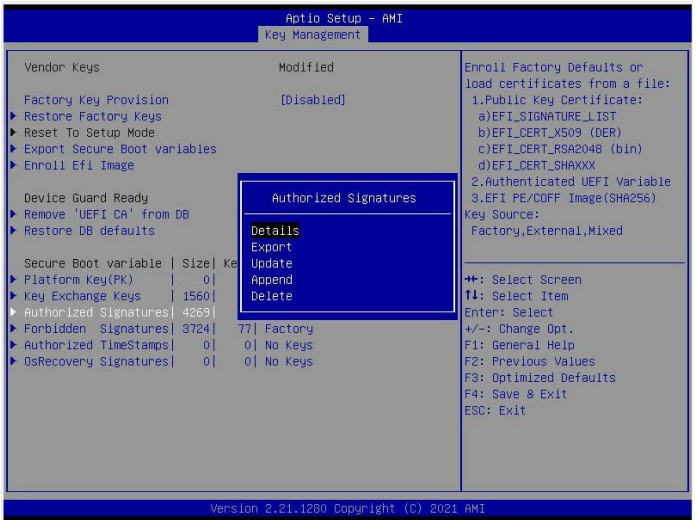


选择No（否），然后按<Enter>从密钥数据库中仅删除一个证书。



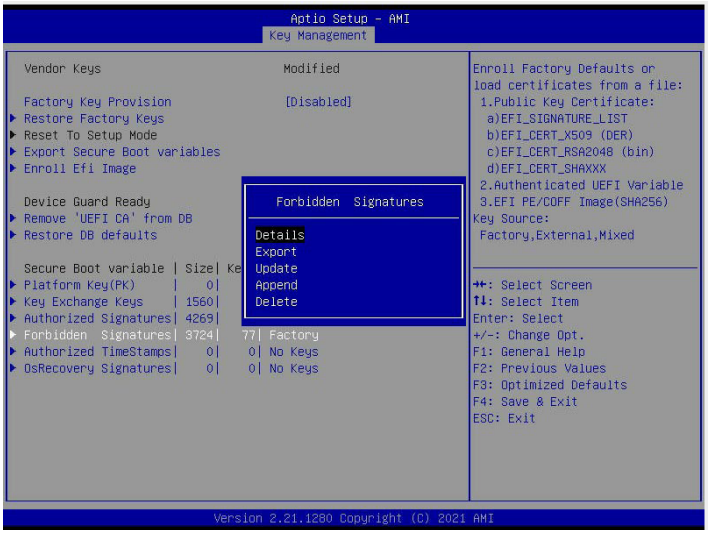
▶Authorized Signatures（授权签名）

授权签名数据库（DB）包含授权签名证书和数字签名。选项有**详细信息**、导出、更新、追加和删除。选择Details（详细信息）显示授权签名的详细信息。选择Export（导出）将当前数据库保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载DB。选择Append（追加）将变量添加到现有数据库。选择Delete（删除）清除当前数据库或仅从密钥数据库中删除一个证书。（有关导出过程，参见第16页。有关更新过程，参见第17、18、19和20页。有关追加过程，参见第21页和第22页。
有关删除过程，参见第23页。）



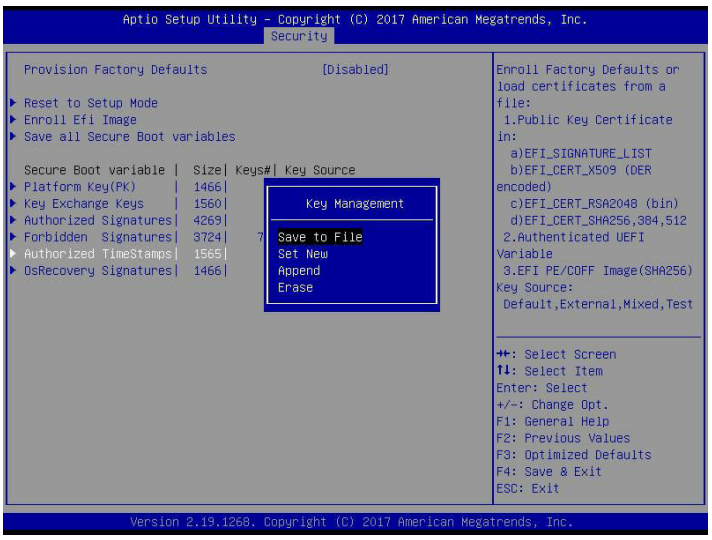
▶Forbidden Signatures（禁止签名）

禁止签名数据库（DBX）包含被禁止的证书和数字签名。选项有**详细信息**、导出、更新、追加和删除。选择Details（详细信息）显示禁止签名的详细信息。选择Export（导出）将当前DBX保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载DBX。选择Append（追加）将变量添加到现有DBX。选择Delete（删除）清除当前DBX，或仅从密钥数据库中删除一个证书。（有关导出过程，参见第16页。有关更新过程，参见第17、18、19和20页。有关追加过程，参见第21页和第22页。
有关删除过程，参见第23页。）



▶Authorized TimeStamps（授权时戳）

授权时戳数据库（DBT）发布并检查已签名的时戳证书。选项有**详细信息**、导出、更新、追加和删除。选择Details（详细信息）显示授权时戳的详细信息。选择Export（导出）将当前DBT保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载DBT。选择Append（追加）将变量添加到现有DBT。选择Delete（删除）清除当前DBT，或仅从密钥数据库中删除一个证书。（有关导出过程，参见第16页。有关更新过程，参见第17、18、19和20页。有关追加过程，参见第21页和第22页。
有关删除过程，参见第23页。）



▶OsRecovery Signatures（操作系统恢复禁止签名）

OsRecovery签名数据库（DBR）包含安全启动授权的恢复变量。选项有**详细信息**、导出、更新、追加和删除。选择Details（详细信息）显示OsRecovery签名的详细信息。选择Export（导出）将当前DBR保存到FAT格式的U盘。选择Update（更新）加载制造商默认值，或从外部设备的文件中加载DBR。选择Append（追加）将变量添加到现有DBR。选择Delete（删除）清除当前DBR或仅从密钥数据库中删除一个证书。（有关导出过程，参见第16页。有关更新过程，参见第17、18、19和20页。有关追加过程，参见第21页和第22页。有关删除过程，参见第23页。）