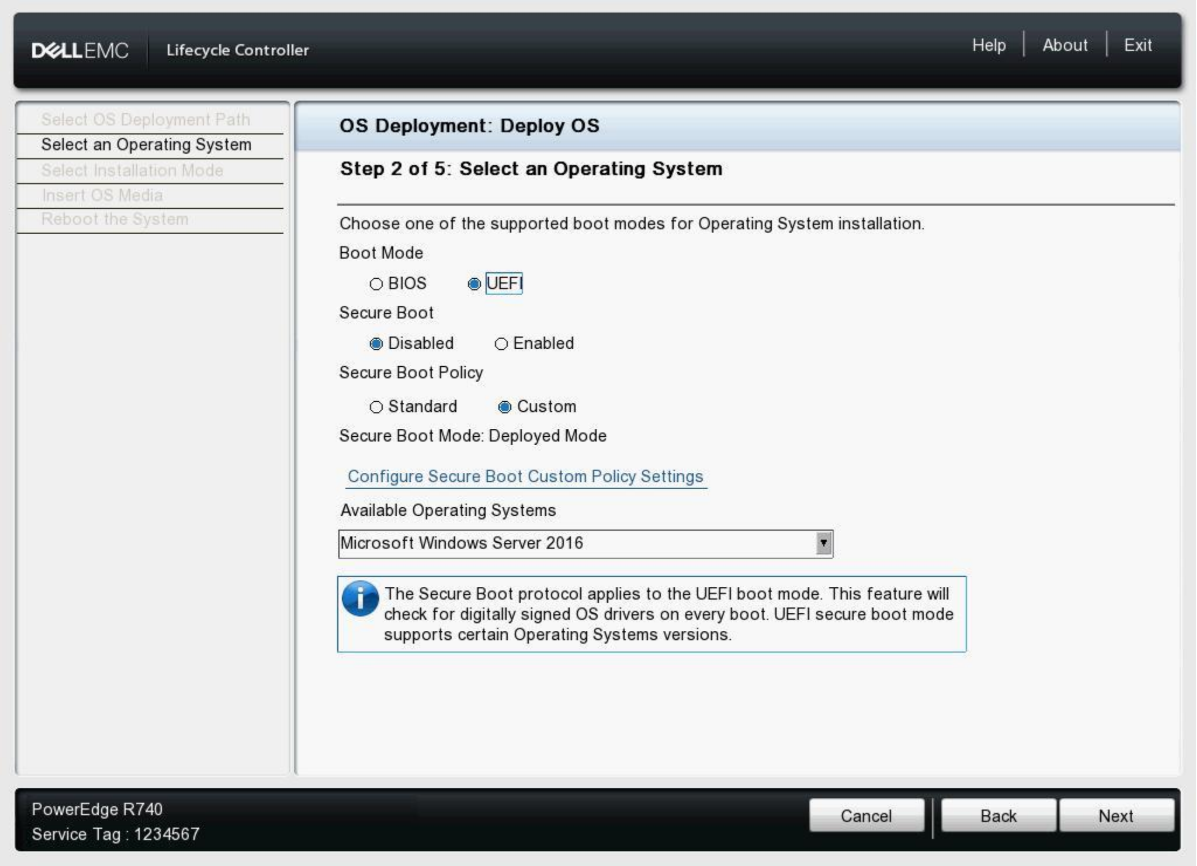
Secureboot certificate management by using LC UI

Secure Boot certificate management feature is supported on the 14th generation and later versions of PowerEdge servers. You can access this feature from various interfaces such as BIOS Settings (press F2 when the company logo is displayed during the POST), Lifecycle Controller graphical user interface (GUI), RACADM, WS-Man, Redfish, and iDRAC GUI. This blog focuses only on Secure Boot certificate management by using Lifecycle Controller GUI.

Lifecycle Controller GUI supports enabling and disabling Secure Boot and allows you to set the secure Boot policy to Standard or Custom. Secure Boot Mode is a read-only option in Lifecycle Controller GUI.

Lifecycle Controller GUI provides the Configure Secure Boot Custom Policy Settings hyperlink which directs you to **Secure Boot Custom Policy Setting** page of the **BIOS Settings** page.

You can perform all the Secure Boot certificate management actions such as View, Export, Import, Delete, Delete All, Reset, and Reset All as though it is performed from the BIOS Settings by pressing F2 when the company logo is displayed while starting the server.



OS Deployment: Deploy OS

Step 2 of 5: Select an Operating System

Choose one of the supported boot modes for Operating System installation.

Boot Mode

○ BIOS ● UEFI

Secure Boot

● Disabled ○ Enabled

Secure Boot Policy

○ Standard ● Custom

Secure Boot Mode: Deployed Mode

Available Operating Systems

Microsoft Windows Server 2016

The Secure Boot protocol applies to the UEFI boot mode. This feature will check for digitally signed OS drivers on every boot. UEFI secure boot mode supports certain Operating Systems versions.

PowerEdge R740
Service Tag : 1234567

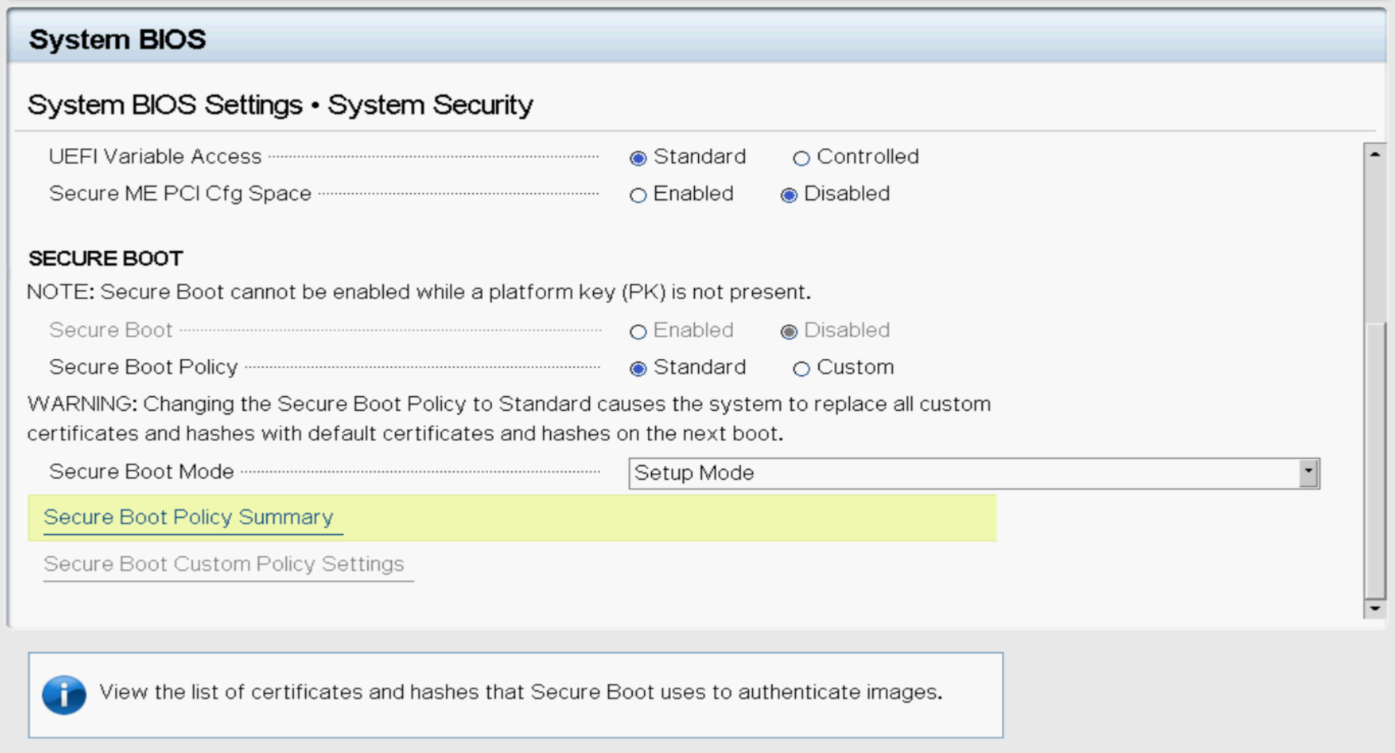
Figure 1. Selecting the boot mode

By default, Secure Boot will be in the *Disabled* mode and the Secure Boot Policy will be set to Standard. If the Secure Boot needs to be made active then the Secure Boot should be configured as *Enabled*. Secure Boot Policy in Standard means that the system will have default certificates and image digests loaded from the factory which will cater to the security of standard firmware, drivers, option-ROMs and boot loader loaded from the factory.

But in case a new driver or firmware to be supported on the machine, the respective certificate must be enrolled into the DB of Secure Boot certificate store. In order to do that, Secure Boot Policy need to be configured to Custom.

When the Secure Boot Policy is configured as Custom, it inherits the standard certificates and image digests loaded in the system by default on which the user can make any modifications, if required. The Secure Boot Policy, configured as Custom, allows you to perform operations such as View, Export, Import, Delete, Delete All, Reset, and Rest All by using which you can configure the Secure Boot policies according to your requirements.

Secure Boot Policy configured as Standard restricts the operations to be performed on the certificate store. Standard Secure Boot Policy restricts the user to view only the certificates—no other actions are allowed on the Certificate Store.



System BIOS

System BIOS Settings • System Security

UEFI Variable Access: ● Standard ○ Controlled

Secure ME PCI Cfg Space: ○ Enabled ● Disabled

SECURE BOOT

NOTE: Secure Boot cannot be enabled while a platform key (PK) is not present.

Secure Boot: ○ Enabled ● Disabled

Secure Boot Policy: ● Standard ○ Custom

WARNING: Changing the Secure Boot Policy to Standard causes the system to replace all custom certificates and hashes with default certificates and hashes on the next boot.

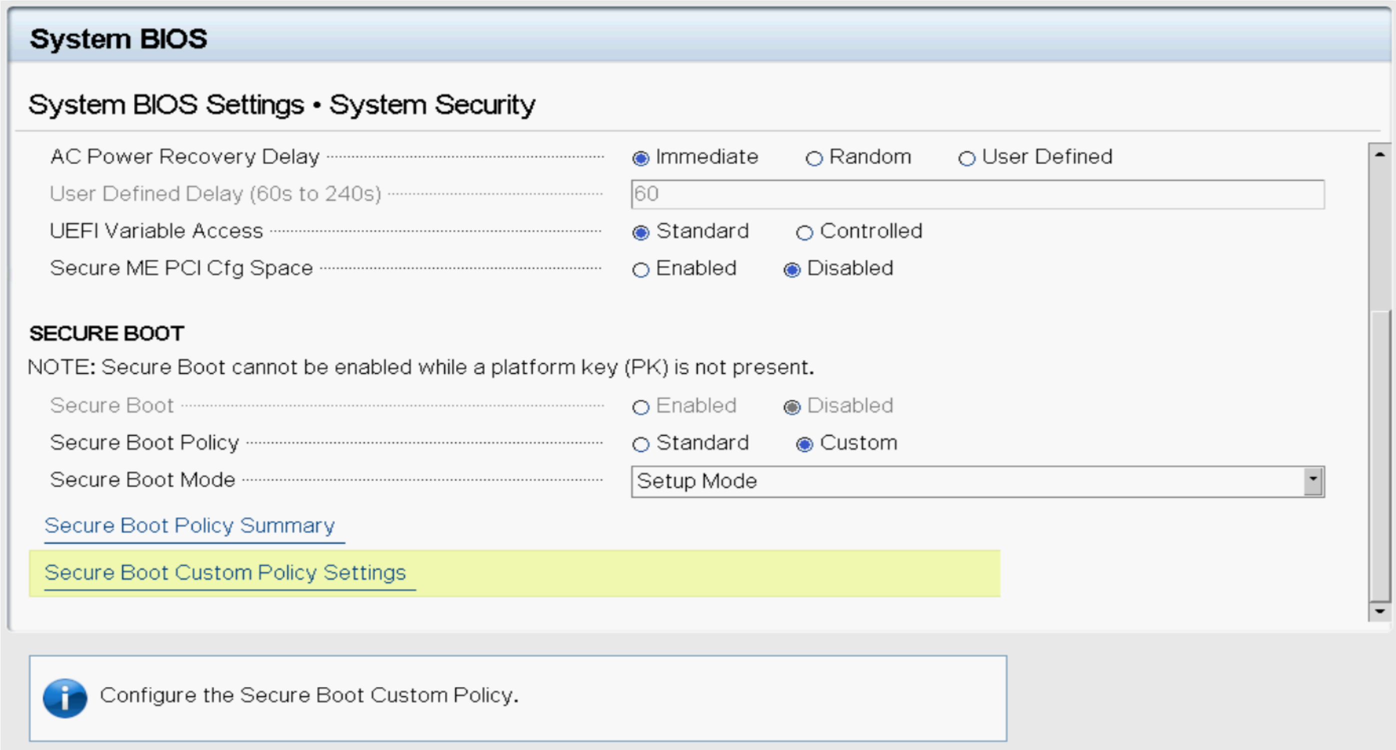
Secure Boot Mode: Setup Mode

Secure Boot Policy Summary

Secure Boot Custom Policy Settings

View the list of certificates and hashes that Secure Boot uses to authenticate images.

Figure 2. Standard Secure Boot policy



System BIOS

System BIOS Settings • System Security

AC Power Recovery Delay ● Immediate ○ Random ○ User Defined

User Defined Delay (60s to 240s) 60

UEFI Variable Access ● Standard ○ Controlled

Secure ME PCI Cfg Space ○ Enabled ● Disabled

SECURE BOOT

NOTE: Secure Boot cannot be enabled while a platform key (PK) is not present.

Secure Boot ○ Enabled ● Disabled

Secure Boot Policy ○ Standard ● Custom

Secure Boot Mode Setup Mode

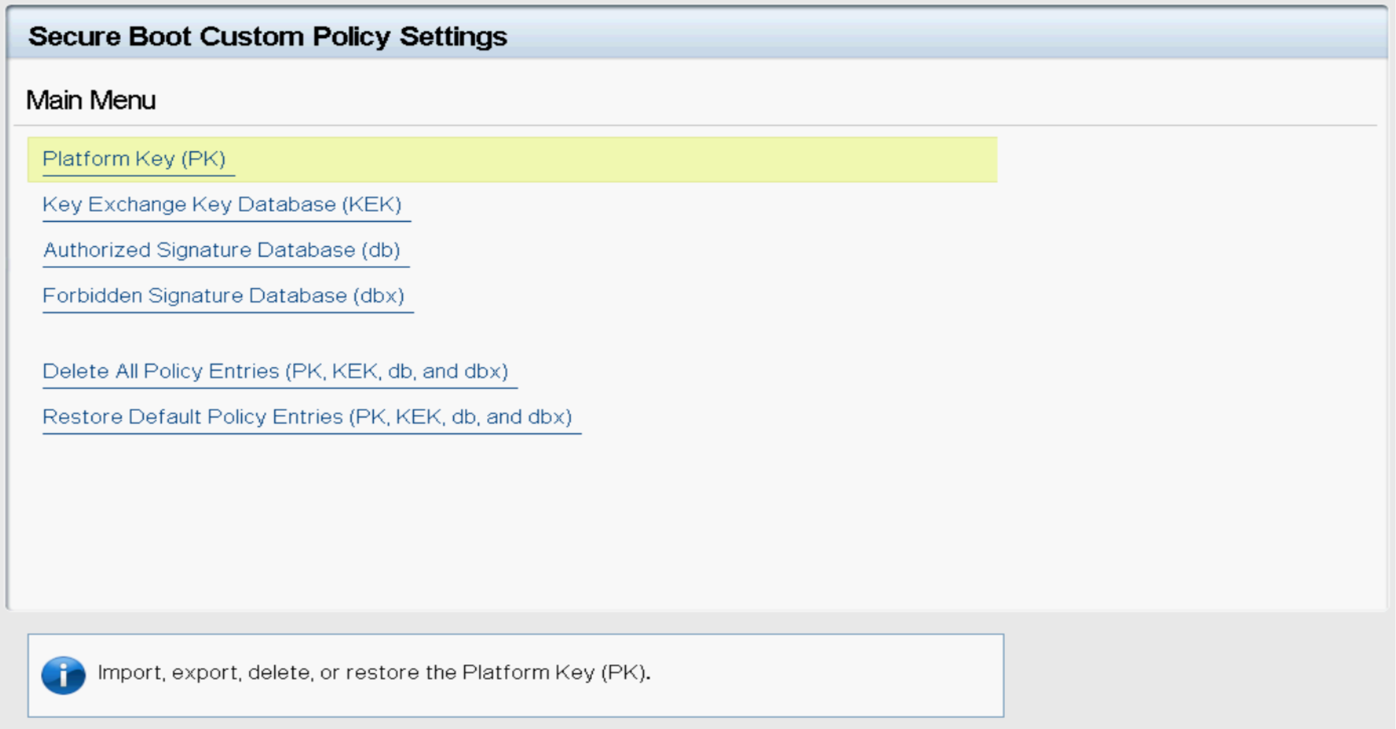
Secure Boot Policy Summary

Secure Boot Custom Policy Settings

Configure the Secure Boot Custom Policy.

Figure 3. Custom Secure Boot policy

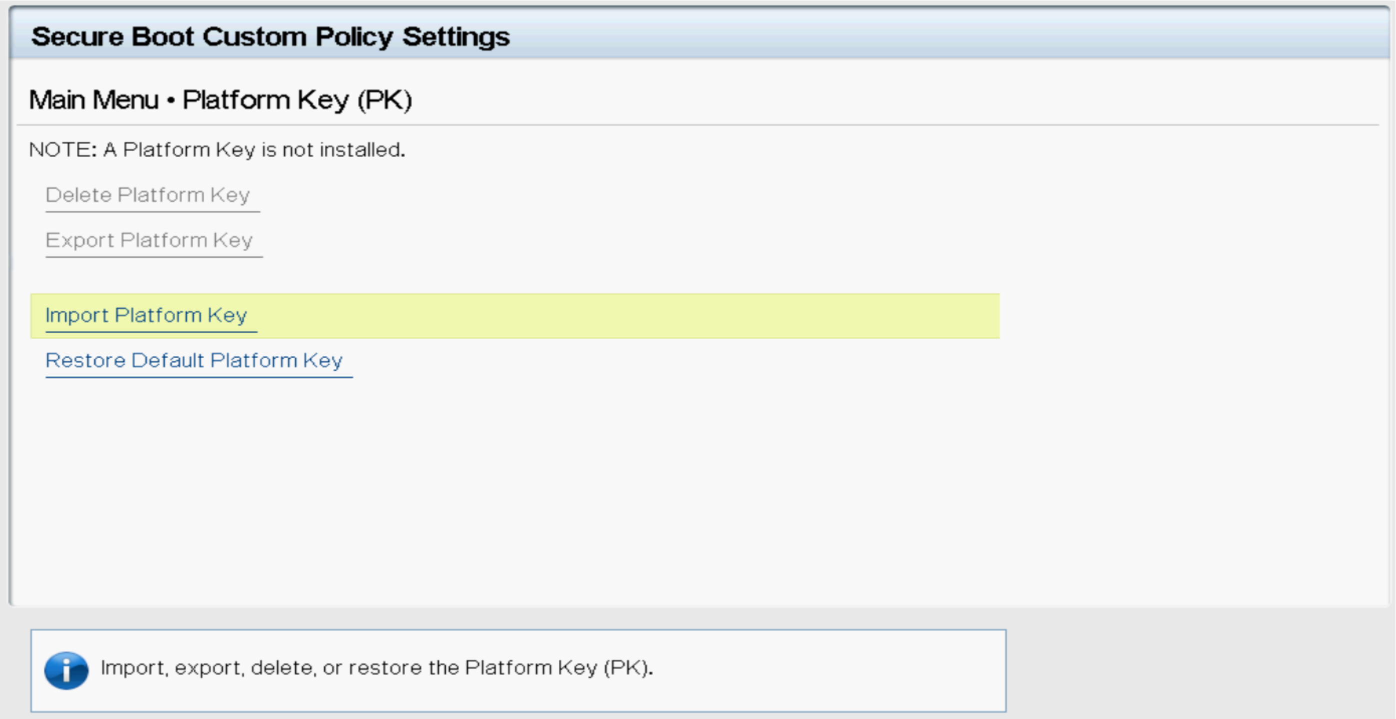
Configuring the Secure Boot Policy to Custom enables the options to manage the certificate store through various actions such as View, Export, Import, Delete, Delete All, Reset, and Rest All on PK, KEK, DB and DBX. User can select the policy (PK / KEK / DB / DBX) on which you want to make the change and perform appropriate actions.


Secure Boot Custom Policy Settings
Main Menu
Platform Key (PK)
Key Exchange Key Database (KEK)
Authorized Signature Database (db)
Forbidden Signature Database (dbx)
Delete All Policy Entries (PK, KEK, db, and dbx)
Restore Default Policy Entries (PK, KEK, db, and dbx)

Import, export, delete, or restore the Platform Key (PK).

Figure 4. Secure Boot Custom Policy Settings-Main menu

Each section will have links to perform Import, Export, Delete, and Reset operations. Links are enabled based on the configuration and what is applicable at the point of time. For example, in the screen shot here, Delete and Export operations are disabled because there is no PK configured yet.



Secure Boot Custom Policy Settings

Main Menu • Platform Key (PK)

NOTE: A Platform Key is not installed.

Delete Platform Key

Export Platform Key

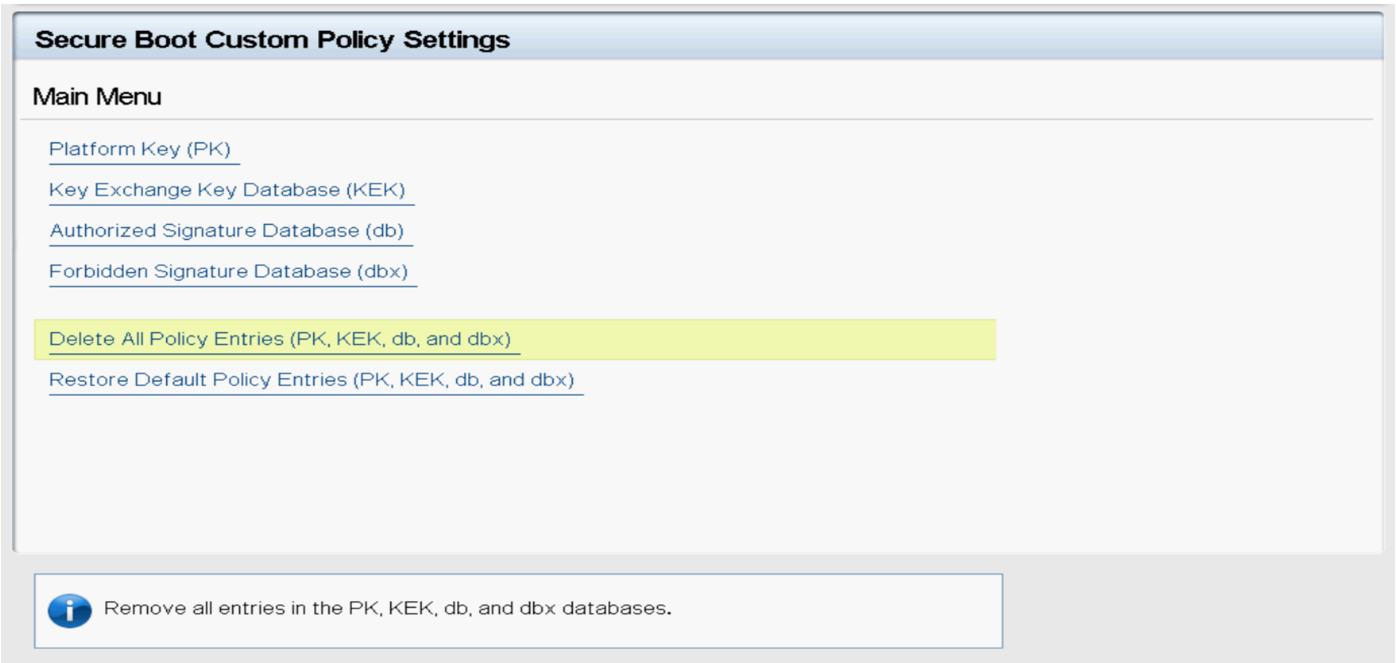
Import Platform Key

Restore Default Platform Key

Import, export, delete, or restore the Platform Key (PK).

Figure 5. Export and Delete Platform Key is disabled

Delete All and *Reset All* are the operations that have impact on all the policies. *Delete All* deletes all the certificates and image digests in the Custom policy, and *Reset All* restores all the certificates and image digests from Standard / *Default* certificate store.



Secure Boot Custom Policy Settings

Main Menu

Platform Key (PK)

Key Exchange Key Database (KEK)

Authorized Signature Database (db)

Forbidden Signature Database (dbx)

Delete All Policy Entries (PK, KEK, db, and dbx)

Restore Default Policy Entries (PK, KEK, db, and dbx)

Remove all entries in the PK, KEK, db, and dbx databases.

Figure 6. Delete All Policy entries