Secure Boot with TPM/vTPM Feature Guide

25.1.2.2

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

Protected by patents, see https://www.ivanti.com/patents.

Contents

Revision History

The following table lists the revision history for this document:

Document Revision	Date	Description
1.0	July 2026	Initial release (OLM release)

Introduction

The Secure Boot feature offers protection against unauthorized bootloader and kernel images, malware, and rootkits, and ensures compliance with secure-by-design principle while improving boot time security validation. This feature is supported on ISA6500/ISA8500 Hardware Appliances for IPS release 25.1.2.2.

Abbreviations Used in This Guide

Term	Description
BIOS and UEFI	Basic input / output system (BIOS) is a program fixed and embedded on a device's microprocessor that helps to initialize hardware operations. Unified Extensible Firmware Interface (UEFI) offers users a faster and sleeker experience. It supports secure booting of the bootloader. BIOS uses 16-bit mode and has a limited user interface, UEFI uses 32-bit or 64-bit mode and offers a more advanced graphical user interface.
MBR and GPT	Master Boot Record (MBR) is the information in the first sector of a hard disk or a removable drive. GUID Partition Table (GPT) is introduced as part of the Unified Extensible Firmware Interface (UEFI) initiative. GPT provides a more flexible mechanism for partitioning disks than the older Master Boot Record (MBR) partitioning scheme.
GRUB and GRUB2	GRand Unified Bootloader (GRUB or GNU GRUB) is a Multiboot boot loader for Linux and other Unix-based OSes. GRUB2 bootloader is the bootloader on x86 systems that is used to load the linux kernel or any other OS. GRUB2 is allowed to load by UEFI if its signature matches the signature in the UEFI's whitelist DB.
IPS	Ivanti Policy Secure (IPS) delivers a robust, scalable network access control (NAC) solution that provides secure, authenticated access for users and devices, ensuring compliance with corporate security policies before granting connectivity to enterprise resources.
ISA	Ivanti Secure Access hardware appliance.

Benefits of Secure Boot Feature

- **Protection from unauthorized bootloader images** - Secure Boot prevents booting unauthorized bootloader (GRUB) images via signature verification of the bootloader (GRUB) from UEFI.
- **Protection from unauthorized kernel images** - Secure Boot prevents booting unauthorized kernel images via signature verification of the kernel from GRUB bootloader.
- **Protection against malware and rootkits** - Secure Boot prevents loading malware/rootkits via chain of trust from UEFI to GRUB to Kernel using signatures verification.
- Compliance with Security By Design principle for boot protection.

Security Best Practices

- Ensure BIOS/UEFI is enabled with Administrative password for every ISA Hardware Appliance. This ensures only authorized Admins can enter BIOS/UEFI settings.
- Ensure **Toggle password protection for the console** is ON for every appliance console access to prevent unauthorized access to Admin console.
- Ensure Secure Boot/vTPM features are always in Enabled state for BIOS/UEFI and VM settings.

Troubleshooting

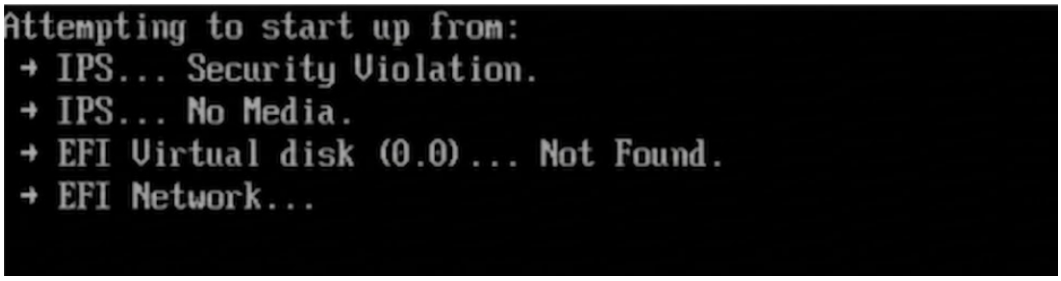
TPM/vTPM is in lockout mode

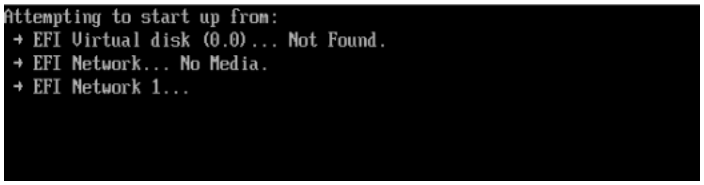
```
1  The TPM is in lockout mode. Please wait till 1000 secs
```

Cause: It could be due to too many consecutive ungraceful shutdowns.

Solution: Once TPM is in lockout state, it will remain inaccessible until the recovery time has elapsed. After 1000 secs, system boots and comes up.

Virtual IPS does not boot due to signature failure

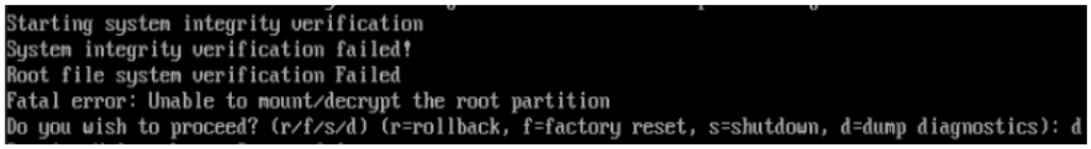




Cause: The primary reason for virtual IPS not booting could be that ExtraConfigs are disabled.

Solution: Enable ExtraConfigs in your VMware settings. For details, see Specifying Advanced Virtual Machine Settings with ExtraConfig Elements.

Booting stops with error "System Integrity verification failed"



Cause: If any new files get created or existing files get modified as part of IPS system, these will be detected and prevent booting.

Solution: Securing InitramFS and RootFS feature prevents unauthorized files creation in IPS system. Select "d" to dump diagnostIPS to see which files are created/modified and Contact Ivanti Support for error. Perform Rollback - option "r" if available or perform Factory Reset – option "f" for clean installation from recovery options provided. All configs will be lost after performing Factory Reset.

Booting stops with error "Rootfs manifest validation related files do not exist"

Cause: If Securing InitramFS and RootFS feature dependent files are missing, the system is interrupted due to failure in validation of required files.

Solution: Contact Ivanti Support for error. Perform Rollback - option "r" if available or perform Factory Reset – option "f" for clean installation from recovery options provided. All configs will be lost after performing Factory Reset.

Booting stops with error "Root file system signature verification failed"

Cause: If Securing InitramFS and RootFS feature dependent file contents are modified, the system is interrupted due to failure in signature verification of required files.

Solution: Contact Ivanti Support for error. Perform Rollback - option "r" if available or perform Factory Reset – option "f" for clean installation from recovery options provided. All configs will be lost after performing Factory Reset.

Booting stops with error "No file entries found in the manifest"

Cause: If Securing InitramFS and RootFS feature dependent files don't have any content, the system is interrupted due to failure in validation of required files.

Solution: Contact Ivanti Support for error. Perform Rollback - option "r" if available or perform Factory Reset – option "f" for clean installation from recovery options provided. All configs will be lost after performing Factory Reset.

Documentation

Ivanti documentation is available at https://www.ivanti.com/support/product-documentation.

Technical Support

When you need additional information or assistance, you can contact "Support Center:

- https://forums.ivanti.com/s/contactsupport
- support@ivanti.com

For more technical support resources, browse the support website
https://forums.ivanti.com/s/contactsupport