CHECKLIST

vSphere Secure Boot and TPM 2.0 Readiness Checklist

A practical checklist to help virtualization teams validate hardware support, firmware settings, boot compatibility, recovery steps, and attestation readiness before enabling Secure Boot and TPM 2.0 in VMware vSphere production environments.

vSphere Secure Boot and TPM 2.0 Readiness Checklist

Use this checklist before enabling Secure Boot and TPM 2.0 on vSphere hosts. It is designed to help you confirm compatibility, reduce rollback risk, and establish a verifiable host-integrity baseline.

---

1) Scope and ownership

- [ ] Identify the hosts in scope for rollout.
- [ ] Confirm whether the change applies to standalone hosts, a cluster, or a staged pilot group.
- [ ] Assign an owner for firmware policy.
- [ ] Assign an owner for host image compatibility.
- [ ] Assign an owner for validation, attestation, or evidence collection.
- [ ] Confirm change approval and maintenance window timing.

---

2) Hardware and firmware prerequisites

- [ ] Confirm the server platform supports UEFI Secure Boot.
- [ ] Confirm the server platform includes TPM 2.0 support.
- [ ] Verify TPM is enabled in system firmware.
- [ ] Verify UEFI boot mode is enabled.
- [ ] Verify legacy BIOS mode is disabled or not used for the target host.
- [ ] Check whether firmware is current and supported for the target vSphere version.
- [ ] Confirm the platform vendor documents Secure Boot and TPM 2.0 support for this model.
- [ ] Verify the host has a documented firmware recovery path.

---

3) Boot chain and image compatibility

- [ ] Confirm the current ESXi image is compatible with Secure Boot.
- [ ] Confirm any custom VIBs, drivers, or boot components are signed and supported.
- [ ] Inventory any unsigned, legacy, or custom boot dependencies.
- [ ] Remove or replace unsupported boot components before rollout.
- [ ] Confirm boot order is correct and stable.
- [ ] Verify the system does not depend on insecure fallback boot paths.
- [ ] Confirm any recovery media or rescue process is compatible with Secure Boot requirements.

---

4) TPM readiness and baseline planning

- [ ] Confirm the TPM is recognized by firmware and the host.

- [ ] Verify whether TPM ownership, clearing, or reinitialization is required before rollout.
- [ ] Decide how you will record the known-good measurement baseline.
- [ ] Define what constitutes acceptable measurement drift.
- [ ] Determine who reviews and approves deviations.
- [ ] Confirm how TPM-related evidence will be retained for audit or incident response.

---

5) Management and operational controls

- [ ] Confirm administrative access to the host is restricted.
- [ ] Confirm physical access to the host is controlled.
- [ ] Confirm remote console access is limited to authorized staff.
- [ ] Verify monitoring is in place for firmware, boot, or host integrity changes.
- [ ] Confirm the change will be logged in your configuration management or ticketing system.
- [ ] Confirm the rollout plan includes rollback or rescue steps.
- [ ] Confirm the team knows how to recover if the host fails to boot.

---

6) Validation before production enablement

- [ ] Test Secure Boot and TPM 2.0 on a non-production or low-risk host first.
- [ ] Reboot the host and confirm it starts normally.
- [ ] Verify the host remains visible and manageable after reboot.
- [ ] Confirm cluster behavior is unchanged if the host is part of a cluster.
- [ ] Validate that hardware inventory, telemetry, or attestation reflects the expected state.
- [ ] Check that no unexpected boot warnings or compatibility errors appear.

- [ ] Record the final settings and validation results.

---

7) Production rollout checklist

- [ ] Schedule rollout during a maintenance window.
- [ ] Ensure backups, snapshots, or rollback plans are appropriate for the environment.
- [ ] Enable Secure Boot on the approved host(s).
- [ ] Enable TPM 2.0 if not already active.
- [ ] Reboot and confirm successful startup.
- [ ] Verify host health, management connectivity, and workload availability.
- [ ] Reconfirm measurement or attestation status after the reboot.
- [ ] Update documentation with the final configuration state.

---

8) Post-change checks

- [ ] Confirm the boot chain is stable after subsequent reboots.
- [ ] Monitor for drift after firmware updates or hardware replacements.
- [ ] Revalidate measurements after any approved change to boot components.
- [ ] Update baselines when legitimate changes occur.
- [ ] Reassess the controls during periodic security reviews.
- [ ] Keep recovery steps current and accessible to operators.

---

9) Common warning signs

Pause the rollout if you see any of the following:

- [ ] The host depends on unsigned or legacy boot components.
- [ ] The recovery workflow fails under Secure Boot.
- [ ] The firmware cannot reliably retain the expected Secure Boot configuration.
- [ ] TPM measurements are unstable without a documented cause.
- [ ] The team cannot explain or approve measurement drift.
- [ ] Recovery media or emergency access is not tested.

---

10) Decision summary

Use Secure Boot and TPM 2.0 when the host is high value, physically exposed, or subject to integrity verification requirements. Be cautious when the environment relies on custom boot tooling, irregular firmware processes, or undocumented recovery paths.

Final go/no-go questions

- [ ] Do we have verified hardware support?
- [ ] Do we understand the boot chain end to end?
- [ ] Do we have a trusted baseline and a way to interpret drift?
- [ ] Do we have a tested rollback and recovery plan?
- [ ] Have we validated this on a non-production host first?

If all answers are yes, the host is a better candidate for production rollout.

Quick reference: what each control does

Control	Primary role	Practical value

Secure Boot	Preventive	Blocks unsigned or tampered boot components from loading
TPM 2.0	Evidentiary	Records boot measurements for later validation or attestation
Together	Preventive + evidentiary	Improves confidence in host boot integrity and supports auditability

---

Notes

- Treat Secure Boot and TPM 2.0 as part of a broader host integrity program.
- Validate compatibility before rollout.
- Document baselines, exceptions, and recovery steps.
- Recheck integrity after firmware updates, hardware replacements, or image changes.