CHECKLIST

ESXi Secure Boot and Lockdown Mode Setup Checklist

A practical checklist for validating VMware ESXi Secure Boot and Lockdown Mode before production rollout, including firmware checks, access planning, recovery preparation, and rollout verification.

ESXi Secure Boot and Lockdown Mode Setup Checklist

Use this checklist to validate whether your ESXi environment is ready to enable Secure Boot, Lockdown Mode, or both. It is designed for production planning, change control, and pre-deployment verification.

---

1) Confirm the host and platform are suitable

- [ ] Confirm the ESXi version and build are supported for the intended security controls.
- [ ] Verify vendor documentation for the exact host hardware model.
- [ ] Confirm firmware support for UEFI Secure Boot on the host platform.
- [ ] Verify that the host boot mode is configured correctly for Secure Boot.
- [ ] Check for any hardware or firmware advisories that could affect boot integrity.
- [ ] Confirm that the host is not dependent on unsupported boot components or custom modifications.

2) Verify the boot chain is ready for Secure Boot

- [ ] Review current firmware settings before making changes.
- [ ] Confirm that Secure Boot can be enabled without breaking the current boot path.
- [ ] Validate that trusted boot components are signed and supported.
- [ ] Confirm that any required vendor extensions, drivers, or agents are compatible.
- [ ] Ensure the host does not rely on unapproved boot-time customizations.
- [ ] Document the expected boot behavior after Secure Boot is enabled.

3) Validate management access before enabling Lockdown Mode

- [ ] Confirm the host can be administered through approved centralized management tools.
- [ ] Verify that remote administration works without relying on direct console access.
- [ ] Test scripted or automated workflows that will be used after Lockdown Mode is enabled.
- [ ] Confirm that authentication and authorization policies support least privilege.
- [ ] Identify all users and service accounts that require legitimate administrative access.
- [ ] Remove or minimize unnecessary direct host access in advance.

4) Define exception handling and recovery paths

- [ ] Document break-glass access procedures.
- [ ] Identify who can approve emergency access and under what conditions.
- [ ] Define how temporary access will be granted, logged, and revoked.
- [ ] Confirm that an out-of-band recovery path exists if centralized management fails.
- [ ] Validate who owns incident response for an inaccessible host.
- [ ] Record rollback steps for both Secure Boot and Lockdown Mode changes.

5) Check logging, auditing, and change control

- [ ] Confirm host and management-plane logging are enabled.
- [ ] Verify that administrative actions are auditable.
- [ ] Ensure change approvals are documented before implementation.
- [ ] Align the rollout with an approved maintenance window.
- [ ] Confirm monitoring will detect failed boots, access errors, or inventory issues.
- [ ] Make sure logs are accessible after reboot and during incident response.

6) Review operational readiness

- [ ] Confirm the operations team understands the new access model.
- [ ] Validate that support runbooks reflect the new controls.
- [ ] Ensure the team knows how to confirm success after reboot.
- [ ] Check that the host can be restored if the configuration causes access problems.
- [ ] Verify that maintenance procedures do not depend on undocumented local changes.
- [ ] Confirm that snapshot, patching, and maintenance workflows are aligned with the new posture.

7) Pilot on a non-critical host first

- [ ] Select a low-risk or non-critical host for the first rollout.
- [ ] Schedule the change during a controlled maintenance window.
- [ ] Enable Secure Boot first if boot-chain validation is the priority.
- [ ] Reboot the host and verify it starts cleanly.
- [ ] Confirm management connectivity after startup.
- [ ] Check that inventory, health data, and alerts are accurate.

8) Enable Lockdown Mode only after validation succeeds

- [ ] Confirm the pilot host is manageable through approved remote paths.
- [ ] Confirm break-glass access works as documented.
- [ ] Enable Lockdown Mode according to your operational policy.
- [ ] Re-test administrative tasks that should still be allowed.
- [ ] Confirm unauthorized direct access is restricted as expected.
- [ ] Validate that support teams can still perform required maintenance tasks.

9) Confirm post-change behavior

- [ ] Reboot again if needed to confirm repeatable boot behavior.
- [ ] Verify the host appears healthy in centralized management.
- [ ] Confirm alerting and logging continue to function normally.
- [ ] Check that monitoring reflects the correct host state.
- [ ] Validate that change records reflect the final configuration.
- [ ] Record any compatibility issues or exceptions discovered during testing.

10) Decide on broader rollout

- [ ] Review results from the pilot host.
- [ ] Confirm no critical management or recovery gaps were found.
- [ ] Update runbooks, diagrams, and access documentation.
- [ ] Train support staff on the new operating model.
- [ ] Approve the rollout plan for remaining hosts.
- [ ] Expand deployment only after validation is complete.

Quick decision guide

Use this rule of thumb:

- Enable Secure Boot now if the platform is supported and the boot path is validated.
- Enable Lockdown Mode now only if remote administration, exception handling, and recovery are proven.
- Delay either control if the host still depends on undocumented local access or untested emergency procedures.

Change record fields to capture

- Host name
- ESXi version and build
- Hardware model
- Firmware/BIOS version
- Secure Boot status before and after
- Lockdown Mode status before and after
- Maintenance window date and time
- Approver name
- Validation results
- Rollback owner
- Notes and exceptions

Final sign-off

- [ ] Security review completed
- [ ] Operations review completed
- [ ] Recovery plan documented

- [ ] Monitoring confirmed
- [ ] Rollback steps tested or reviewed
- [ ] Production deployment approved

Result: If every required check is complete, the environment is ready for controlled production rollout of Secure Boot, Lockdown Mode, or both.