



TEMPLATE

Hyper-V Secure Boot Configuration Checklist and Template

A practical one-page template for validating Hyper-V Secure Boot settings before production use, including generation, guest compatibility, template selection, verification steps, and rollback notes.

Hyper-V Secure Boot Configuration Template

Use this template to document and validate Secure Boot for a Hyper-V virtual machine before production deployment.

1) VM Identification

- VM name: _____
- Owner / team: _____
- Environment: ? Dev ? Test ? Staging ? Production
- Date reviewed: _____
- Reviewer: _____

2) Baseline Compatibility Check

- VM generation: ? Generation 2 ? Generation 1
- Guest OS / distribution: _____
- Guest version / build: _____



- UEFI Secure Boot supported by guest: ? Yes ? No ? Confirmed by vendor documentation
- Legacy boot dependency present: ? No ? Yes
- Custom unsigned boot components present: ? No ? Yes

Decision:

- ? Secure Boot is appropriate
- ? Secure Boot requires exception review
- ? Secure Boot should remain disabled

3) Secure Boot Configuration

- Secure Boot enabled: ? Yes ? No
 - Template selected: _____
 - Reason for template choice: _____
-

Template guidance

- Windows guests: typically use the Microsoft template.
- Linux guests: typically use the Linux-oriented template that matches the guest signing model.
- Appliances / specialty OS: verify vendor support before enabling.

4) Validation Checklist

Complete these checks after configuration:

- ? VM is confirmed as Generation 2
- ? Guest OS support is verified
- ? Correct Secure Boot template is selected



- ? VM boots successfully with Secure Boot enabled
- ? Boot sequence completes without firmware or bootloader errors
- ? Guest OS loads normally and remains manageable
- ? Configuration is recorded in build / change documentation
- ? Rollback path is documented and available

5) Production Readiness Review

Mark each item before promoting the VM to production:

- ? Secure Boot setting matches the workload design
- ? Backup / recovery plan has been reviewed
- ? Host access controls are in place
- ? Network segmentation is documented
- ? Image version and template are standardized
- ? Any exception is approved and recorded

6) Change Control Notes

- Change ticket / record: _____
- Rollback method: _____
- Notes / exceptions:

7) Quick Decision Rule

Use this rule of thumb:



> Enable Secure Boot on Generation 2 VMs unless the guest explicitly requires it off. Match the template to the guest OS family, then validate the boot path before production.

Sign-off

- Approved by: _____
- Date: _____
- Status: ? Approved ? Needs review ? Rejected