STIG-Compatibility-Report-PUBLIC

STIG Compatibility Report

AA-HUD (Acacia Avenue Heads-Up Display)

Vendor: Acacia Avenue LLC
Website: www.acaciaave.com
Product: AA-HUD — Acacia Avenue Heads-Up Display
Version Tested: v1.0.067.4
Report Date: March 11, 2026
Benchmark: DISA Windows 11 STIG V2R7 (January 2026)
SCAP Tool: SCAP Compliance Checker (SCC) 5.14 — NIWC Atlantic

---

Executive Summary

> ✅ **AA-HUD introduces zero new STIG findings** when installed on a STIG-hardened Windows 11 workstation under Group Policy management.

Installation and operation of AA-HUD does not alter the STIG compliance posture of a Windows 11 endpoint. Organizations operating under STIG-mandated baselines can deploy AA-HUD with confidence that their compliance status is unaffected.

Test Environment

Component	Details
Operating System	Windows 11 Enterprise, Version 25H2
Domain	Isolated Active Directory test domain (Windows Server 2025)
STIG Benchmark	DISA Windows 11 STIG V2R7, January 2026
SCAP Tool	SCAP Compliance Checker (SCC) 5.14 — NIWC Atlantic
HUD Deployment Method	Group Policy (ADMX/ADML templates)
HUD Version	v1.0.067.4

Environment notes:

- Fresh OS installation with no pre-existing third-party software
- Full DISA Windows 11 STIG GPO baseline applied via Group Policy prior to baseline scan
- AA-HUD settings configured via Group Policy using vendor-supplied ADMX/ADML templates

- AA-HUD installed via MSI (`HeadsUpDisplay.Setup.msi`) under standard administrator credentials

---

Methodology

Testing followed a controlled before/after scan methodology:

1. Built a clean Windows 11 Enterprise workstation, domain-joined to an isolated test Active Directory environment
2. Applied the full DISA Windows 11 STIG GPO baseline via Group Policy
3. Ran **SCC pre-installation scan** — established STIG compliance baseline with no HUD present
4. Deployed HUD ADMX/ADML templates to the Group Policy Central Store; created and linked HUD GPO with representative production settings; verified via `gpresult /r`
5. Installed AA-HUD via MSI; rebooted; confirmed HUD displays correctly under GPO configuration
6. Ran **SCC post-installation scan** — recorded all findings with HUD installed and active
7. Compared pre- and post-installation reports — identified any delta introduced by AA-HUD

Results

The following table summarizes findings from the DISA Windows 11 STIG V2R7 benchmark across both scans. Findings shown are those present on the baseline OS regardless of HUD installation; they are not introduced by AA-HUD.

Severity	Pre-Installation	Post-Installation	Delta
CAT I — High	12	12	**0**
CAT II — Medium	127	127	**0**
CAT III — Low	9	9	**0**
Total	**148**	**148**	**0**

> **AA-HUD introduced zero new findings in any category.**

Note: Baseline findings (148 total) are standard OS-level STIG items present on any freshly deployed Windows 11 workstation prior to full manual STIG remediation (e.g., BitLocker configuration, DoD Root CA certificate installation, account renaming). They are unrelated to AA-HUD.

What AA-HUD Installs

The following components are deployed by the AA-HUD MSI and were evaluated during testing:

Component	Description	STIG Impact
`aahud.exe`	Core HUD process (native C++ application)	None
Scheduled Task	Launches `aahud.exe` at user logon	None
`HKLM\SOFTWARE\AcaciaAve\HUD`	Configuration registry keys	None
`HKLM\SOFTWARE\Policies\AcaciaAve\HUD`	GPO-managed policy registry keys	None

Compatibility Notes

AppLocker / WDAC (Application Whitelisting)
If application whitelisting is enforced via AppLocker or Windows Defender Application Control (WDAC), `aahud.exe` must be added to the allow list. This is standard practice for any third-party application in a whitelisting environment and does not represent a STIG finding.

Scheduled Task
The logon task created by the AA-HUD installer complies with STIG scheduled task configuration requirements.

Network Activity
AA-HUD does not open network ports or make outbound connections during normal operation. It functions entirely as a local display application reading configuration from Group Policy registry values.

Runtime Dependencies
AA-HUD requires the Microsoft Visual C++ Redistributable runtime as a prerequisite. It must be deployed separately prior to AA-HUD installation. This runtime is published by Microsoft, is widely pre-installed on enterprise workstations, and introduces no STIG findings. It can be deployed via Group Policy or included as a prerequisite step in enterprise software distribution tooling (e.g., SCCM, Intune).

Conclusion

AA-HUD v1.0.067.4 is fully compatible with the DISA Windows 11 STIG V2R7 benchmark. Controlled before/after testing using SCAP Compliance Checker 5.14 confirmed that AA-HUD installation introduces **zero new CAT I, CAT II, or CAT III findings**.

AA-HUD can be deployed on STIG-hardened Windows 11 endpoints without affecting the organization's STIG compliance posture.

References

- DISA STIG Downloads
- SCAP Compliance Checker (SCC) — NIWC Atlantic
- AA-HUD Product Page
- AA-HUD GitHub Repository

This report reflects testing performed by the vendor, Acacia Avenue LLC. Independent verification is encouraged. Raw SCC scan data (pre- and post-installation XCCDF results, HTML reports, and DISA CKL files) is available upon request. Contact sales@acaciaave.com with questions.