# Q3 2026 Release Notes

| | | | |
|---|---|---|---|
| DOCUMENT | Quarterly Release Notes | PACKAGE | 2026Q3 |
| APPLIES TO | StigSanctum 2.3.0 and later | AUDIENCE | System administrators, ISSOs |

This release incorporates the DISA STIG updates from the July 2026 quarterly release cycle. DISA updated 21 of the STIG publications covered by StigSanctum, adding 15 new StigIDs, revising 751, and retiring 45.

**751**
STIGID UPDATES

**37**
BENCHMARK UPDATES

**15**
NEW STIGIDS

**45**
RETIRED STIGIDS

## STIG Sunset Notices

### Newly Sunset This Quarter

DISA moved two STIGs to **Sunset** status in the July 2026 release:

- **Microsoft Windows Server 2019** (V3R9)
- **Microsoft .NET Framework 4.0** (V2R9)

Sunset STIGs are no longer expected to receive quarterly updates from DISA. **StigSanctum continues to support and scan both benchmarks.** Sunset benchmarks include DISA's sunset check that flags systems still running the sunset technology. We recommend you upgrade when possible.

## DISA STIG Updates (July 2026)

The following summarizes key changes from DISA's quarterly STIG release for Q3, July 2026.

## Microsoft Windows Server 2025 - V1R2

> **New OpenSSH StigIDs**
>
> DISA added 11 new StigIDs (**WN25-SH-000010** through **WN25-SH-000110**) securing the optional OpenSSH server: service state, DOD logon banner, public key authentication, blank password denial (CAT I), session key renegotiation, unresponsive-session termination, configuration and host key file permissions, and GSSAPI restrictions. All 11 are fully automated in StigSanctum and are Not Applicable when OpenSSH isn't installed.

- **WN25-AU-000581 / 000582 / 000584** - File system and handle manipulation auditing requirements removed due to operational issues.
- **WN25-00-000090** - TPM requirement now applies to all systems; the standalone-system exemption was removed.
- **WN25-00-000250** - Data-at-rest encryption raised to CAT I, with a new Not Applicable path for documented hypervisor or storage-array encryption.
- **WN25-PK-000010** - DOD Root CA 4 removed from the required certificate list.
- **WN25-AU-000060** - Not Applicable for Server Core installations.

## Microsoft Windows 11 - V2R8

- **WN11-00-000250**, **WN11-AU-000581 / 000582 / 000584**, **WN11-CC-000065**, **WN11-CC-000197** - StigIDs removed due to operational issues or technical changes in Windows 11.
- Ten checks now document the Group Policy and the Intune-managed registry locations; StigSanctum accepts either location.
- **WN11-00-000010**, **WN11-CC-000075** - TPM and Credential Guard requirements now apply to all systems; standalone and VDI exemptions were removed.
- **WN11-PK-000005 / 000010** - DOD Root CA 4 removed; ECA Root CA 5 added to the accepted certificate list.

## Microsoft Windows Server 2022 - V2R9 / Server 2019 - V3R9

- **WN22-AU-000581 / 000582 / 000584** - Auditing requirements removed due to operational issues.
- **WN22-00-000090** - TPM requirement now applies to all systems.
- **WN22-00-000250** - New Not Applicable path for documented hypervisor or storage-array encryption.
- **WN22-PK-000010** - DOD Root CA 4 removed from the required certificate list.
- **WN19-00-000100** - Windows Server 2019 STIG moved to Sunset status (see Sunset Notices above).

## Red Hat Enterprise Linux 8 - V2R8

- **RHEL-08-040221 / 040222** - New requirements to log IPv4 packets with impossible addresses (martian packets).
- **RHEL-08-040287** - Reverse path filtering requirement for the default IPv4 interface setting restored to the STIG.
- **RHEL-08-010490**, **RHEL-08-030610** - SSH private host key and audit configuration file permissions tightened from 0640 to 0600.
- **RHEL-08-020060** - GNOME session idle lock threshold reduced from 15 to 10 minutes.
- **RHEL-08-010371** - Package signature verification (gpgcheck) alignment across distributions.

## Red Hat Enterprise Linux 9 - V2R9

- **RHEL-09-654097** and nine related audit requirements - Audit rules updated in accordance with Red Hat recommendations, including execve-based auditing of cron-executed commands.
- **RHEL-09-255120**, **RHEL-09-653110** - SSH host key and audit configuration permissions tightened to 0600.
- **RHEL-09-255130** - SSH compression requirement removed.
- **RHEL-09-215015** - FTP server check updated to target the vsftpd package.

## Red Hat Enterprise Linux 10 - V1R2

- **RHEL-10-700750** - GNOME session idle lock threshold reduced to 10 minutes.
- **RHEL-10-600750** - Password hashing requirement updated to sha512.
- **RHEL-10-500410** - Kernel module auditing updated to the init_module and finit_module system calls.
- **RHEL-10-200691** - Postfix alias map verification updated to the lightning memory-mapped database format.

## Canonical Ubuntu 22.04 LTS - V2R9 / 24.04 LTS - V1R6

> **Severity Change**
>
> **UBTU-22-215040** - NFS server package prohibition reclassified from CAT I to CAT II, and the check narrowed to the nfs-kernel-server package only, with a new Not Applicable path for authorized NFS use.

- **UBTU-22-271025** - Graphical session lock threshold reduced from 15 to 10 minutes.

- **UBTU-22-432010** - Sudo reauthentication check narrowed to the !authenticate directive; NOPASSWD entries are no longer flagged by this requirement.
- SSH service restart commands modernized across twelve fix procedures in both releases.

### Microsoft Defender Antivirus - V2R9

- **WNDF-AV-000054** renumbered to **WNDF-AV-000100** so the exclusion-hiding requirement is applied last. StigSanctum carries prior scan history forward under the new number.
- **WNDF-AV-000005 / 000006 / 000007** - Notes added explaining interaction with the exclusion-hiding setting.

### Cisco IOS Router / Switch NDM - V3R8

- **CISC-ND-000090 / 000100 / 000110 / 000120 / 000330 / 000880 / 001250 / 001270** - Eight account and privilege auditing requirements consolidated into **CISC-ND-000210** on the IOS Router and IOS Switch NDM STIGs.
- **CISC-ND-001370** - Redundant authentication server example syntax updated.
- **CASA-ND-001350** (Cisco ASA) - Automatic configuration backup example updated to syslog event ID matching.

### Juniper EX Switches - Y26M07

- **JUEX-L2-000120 / 000130 / 000140** - DHCP snooping, IP Source Guard, and Dynamic ARP Inspection requirements clarified to apply to VLANs with active access interfaces.
- **JUEX-NM-000600** - Audit offload requirement simplified to external syslog forwarding.

### IIS 10.0, DNS, Firefox, and Others

- **IIST-SI-000270** - HTTP Server header suppression registry value changed from 2 to 1.
- IIS 10.0 - **IIST-SV-000115** and **IIST-SV-000139** retired; six site requirements gained broader Not Applicable conditions for SharePoint, WSUS, and Exchange hosts.
- Windows Server DNS - **WDNS-22-000039 / 000040 / 000043** now Not Applicable for servers hosting only Active Directory-integrated zones.
- Mozilla Firefox - **FFOX-00-000038** (Pocket) retired as deprecated.
- Internet Explorer 11 - Sunset requirement wording revised for operating systems under extended support.

## Retired StigIDs

DISA retired 45 StigIDs across 13 Benchmarks this quarter. The largest change was from the Cisco IOS Router and Switch NDM auditing consolidation. StigSanctum will not scan retired StigIDs, but findings generated for them from prior scans are maintained in the scan history for audit purposes.

## StigSanctum Scan Updates

Scan coverage was updated to match the revised DISA check content:

- **Windows Server 2025 OpenSSH checks** - Eleven new automated checks cover the new OpenSSH StigIDs end to end, including configuration keyword verification, file and host key permission analysis, and service state. All are automatically Not Applicable when OpenSSH isn't installed.
- **DOD and ECA root certificate checks** - Certificate validation was updated for DISA's retirement of DOD Root CA 4: Windows Server 2022/2025 and Windows 11 no longer require it, while Windows Server 2019 retains its published list. The ECA check now accepts any valid, unexpired ECA Root CA per the revised guidance.
- **Linux audit rule and permission checks** - RHEL 9 audit rule verification accepts either DISA-published rule syntax, cron auditing follows the new execve-based rules, and permission thresholds for SSH host keys and audit configuration were tightened to 0600 on RHEL 8 and 9. GNOME session lock checks now enforce the 10-minute threshold on RHEL 8, RHEL 10, and Ubuntu 22.04.
- **Intune-managed Windows 11 support** - Five Windows 11 checks whose settings live in a different registry location under Intune management now verify the Group Policy and Intune locations, preventing false findings on Intune-managed endpoints.
- **False-positive reductions** - The Ubuntu sudo reauthentication check no longer flags NOPASSWD entries, and the Ubuntu NFS check no longer flags the nfs-common client package - matching DISA's narrowed requirements. The Juniper audit offload check was simplified to match the reduced requirement.

### Additional DISA Changes Reviewed

Approximately 500 additional revisions were reviewed and confirmed to be editorial - registry path formatting, example refreshes, and typo corrections - requiring no scan changes. Cisco administrator activity logging and redundant authentication server checks were verified as already aligned with the revised check content.

## Platform Improvements

Enhancements shipped since the Q2 2026 release:

### Scheduled Scans

- A new Scheduled Scans page in the web dashboard makes recurring scans easier to set up - create and manage SQL Server Agent scan jobs without leaving the browser
- Unattended scan jobs run under a dedicated service account with least-privilege grants configured by the installer

### Role-Based Access Control

- Access control was strengthened and validated end to end: data-modifying operations are verified against security group membership and recorded in the audit log
- Read access is scoped to each user's benchmark assignments across the dashboard
- Upgrades preserve database users, roles, and memberships

### Network Device Scanning Reliability

- Cisco and Juniper scans reuse a single SSH session with connection pre-flight checks, clearer failure reporting, and full support for DOD login banners on hardened devices
- Command rejections now have better error handling and are saved as findings rather than NaF
- The Juniper SRX SNMP version check now correctly flags SNMPv1 and SNMPv2c configurations as findings

## Upgrade Instructions

#### Upgrade Steps

1. Back up your StigSanctum database
2. Run the installer and select the Upgrade option
3. Update the StigSanctum PowerShell module on any remote scan servers
4. Verify scan results on test systems before production rollout

#### Notes for This Upgrade

- Two severity reclassifications: **`WN25-00-000250`** raised to CAT I, **`UBTU-22-215040`** lowered to CAT II. Prior findings retain their historical severity in scan history.
- Systems running .NET Framework 4.x will report a new open finding from the .NET sunset requirement; disposition per your organization's migration plan.

- Findings for the 45 retired StigIDs are preserved in scan history but will no longer appear in new scans or checklists.

## Support

For questions or issues related to this release:

- Email: **support@stigsanctum.com**
- Release Notes: **www.stigsanctum.com/release-notes.html**