Q4 2026 Release Notes

DOCUMENT	Quarterly Release Notes	PACKAGE	2026Q4
APPLIES TO	StigSanctum 2.3.0 and later	AUDIENCE	System administrators, ISSOs

This release incorporates the DISA STIG updates from the October 2026 quarterly release cycle. DISA updated 24 of the benchmarks covered by StigSanctum, adding 17 new StigIDs, revising 184, retiring 11, and renumbering one.

184
STIGID UPDATES

24
BENCHMARK UPDATES

17
NEW STIGIDS

11
RETIRED STIGIDS

STIG Sunset Notices

⚠ Newly Sunset This Quarter

DISA moved three STIGs to **Sunset** status in the October 2026 release:

- **Red Hat Enterprise Linux 8** (V2R9)
- **Microsoft Exchange 2016 Edge Transport Server** (V2R7)
- **Microsoft Exchange 2019 Edge Server** (V2R3)

DISA no longer issues quarterly updates for sunset STIGs. **StigSanctum still supports and scans all three benchmarks.** The two Exchange Edge benchmarks have a new CAT I StigID that flags Exchange versions Microsoft no longer supports. We recommend upgrading when you can.

🔑 Maximum Password Age Moves to 180 Days

📅 Largest Change This Quarter

DISA raised the maximum password age from 60 to 180 days on Windows 11, Windows Server 2022 and 2025, RHEL 8, 9, and 10, and Ubuntu 22.04 and 24.04. StigSanctum scans and remediation now use the 180-day value on these benchmarks. **Windows Server 2019 remains at 60 days** because DISA didn't change it, and StigSanctum applies each benchmark's value when run on the same system.

🛡️ DISA STIG Updates (October 2026)

The following summarizes key changes from DISA's quarterly STIG release for Q4, October 2026.

Microsoft Windows 11 - V2R11

- `WN11-00-000400` - New: all Wi-Fi Direct adapters must be disabled.
- `WN11-CC-000366` - New: Windows apps must not be activated by voice.
- `WN11-00-000040` - The supported servicing level check now uses Microsoft's end-of-support dates. Windows 11 23H2 reaches end of support on November 10, 2026.
- `WN11-SO-000080` - Retired.

Microsoft Windows Server 2025 - V1R4 / Server 2022 - V2R11

- `WN25-00-000480` - New: Windows Server 2025 must be maintained at a supported servicing level.
- `WN22-00-000100` - The supported servicing level check now uses Microsoft's end-of-support dates.
- `WN22-00-000020`, `WN25-00-000020` - The built-in Administrator password check now also covers the required Windows LAPS configuration on domain members.
- `WN22-DC-000405`, `WN25-DC-000405`, `WN22-SO-000140`, `WN25-SO-000140` - Retired.

Red Hat Enterprise Linux 8 - V2R9, 9 - V2R10, 10 - V1R3

- `RHEL-08-010293`, `RHEL-09-672055`, `RHEL-10-300085` - New CAT I: approved encryption must be implemented in the OpenSSL package.
- `RHEL-08-010287` - New CAT I: the SSH daemon must use systemwide crypto policies.

- **RHEL-08-030565**, **RHEL-09-654176**, **RHEL-10-500605** - New: uses of the useradd command must be audited.
- **RHEL-09-171011** renumbered to **RHEL-09-271011** (graphical logon banner).
- **RHEL-08-010471**, **RHEL-09-215030**, **RHEL-09-215065**, **RHEL-10-200050** - Retired.

Canonical Ubuntu 22.04 LTS - V2R10 / 24.04 LTS - V1R7

> ⇄ **Severity Changes**
>
> **UBTU-22-231010** and **UBTU-24-600090** - Data-at-rest encryption raised from CAT II to CAT I.

- **UBTU-22-654126**, **UBTU-24-900315** - New: uses of the useradd command must be audited.
- **UBTU-22-412040**, **UBTU-24-101100** - New: system accounts must not have an interactive login shell.
- **UBTU-22-654240** - New: audit rules must be protected from unauthorized change.
- **UBTU-24-200680** - Retired.

Microsoft Defender Antivirus - V2R10

- Twelve requirements now document an Intune-managed registry location in addition to Group Policy.

Microsoft IIS 10.0 Server - V3R8 / Site - V2R17

- **IIST-SI-000270** - The HTTP Server header value may now be 1 or 2.
- **IIST-SV-000160** - SMTP relay requirement now includes third-party relays.
- Eighteen site requirements gained Not Applicable conditions for Office Online Server hosts.

Cisco IOS Router and Switch NDM - V3R9

- **CISC-ND-000010** - The example configuration for limiting concurrent management sessions was revised.

Active Directory, DNS, Azure SQL Database, and Firefox

- Active Directory Domain (V3R8) - **AD.0001** group names revised.
- Windows Server DNS (V2R6) - **WDNS-22-000046** now covers IPv6 addressing; **WDNS-22-000094** retired.
- Azure SQL Database (V2R4) - **ASQL-00-010900** audit storage requirement revised.

- Mozilla Firefox (V6R9) - **FFOX-00-000016** DOD Root CA 4 removed from the required certificate list.

Retired StigIDs

DISA retired 11 StigIDs across 8 benchmarks this quarter. StigSanctum no longer scans retired StigIDs, and they don't appear in new checklists. On upgrade, findings for retired StigIDs, including those from earlier releases, are removed from active findings and remain in scan history.

StigSanctum Scan Updates

Scan coverage was updated to match the revised DISA check content. **These changes can alter results even on systems you haven't changed:**

- **Windows LAPS on Server 2022 and 2025** - Domain members without the required LAPS policy now report an open finding on the Administrator password StigIDs.
- **Domain controller data file shares** - **WN19-DC-000120**, **WN22-DC-000120**, and **WN25-DC-000120** now evaluate hidden user shares. Domain controllers with user shares on the directory data drive may report new open findings.
- **Defender Antivirus Intune settings** - Twelve checks now evaluate the Group Policy and Intune locations. A disallowed value in either is a finding.
- **Interoperability cross-certificates** - **WN22-PK-000020**, **WN22-PK-000030**, and their Windows Server 2025 equivalents now require a valid, unexpired certificate.
- **Per-user settings** - Checks of per-user settings now read every loaded profile, and flag any enabled account whose profile isn't loaded so you can review it manually.
- **Linux authentication and packages** - **RHEL-08-020101** now requires the password complexity module to be set as `required`. **RHEL-10-200730** now reports a finding when the pkcs11-provider package is missing.
- **Cisco IOS session limits** - **CISC-ND-000010** on IOS Router and Switch NDM now requires `ip http max-connections` or VTY lines limited as DISA shows. A standard `line vty 0 4` or a `session-limit` no longer passes. IOS-XE and IOS-XR are unchanged.

Additional DISA Changes Reviewed

Approximately 760 additional revisions changed only rule identifiers or terminology and required no scan changes. DISA's text now refers to the Department of War and "DoW". We kept DISA's wording where DISA published it; StigSanctum's check names, comments, and remediation guidance still say DoD.

Platform Improvements

Enhancements shipped since the Q3 2026 release:

Scan Accuracy and Speed

- Network device checks were corrected for storm control, OSPF authentication, bogon lists, PIM, LDP, RSVP, and SSH connection limits, so results on network devices may change
- Nine logon banner checks now verify the banner text rather than only its presence
- Windows Server security policy checks share one policy export per scan, which reduces scan time

Findings and Dashboard

- Comment options now cover more of the conditional Not Applicable paths that DISA defines, across all benchmarks
- The findings page gained sorting and tooltips, and the Recent Changes view loads faster
- Remediation now checks for elevation up front and reports one clear message
- The database now keeps a reference of StigIDs that DISA renumbers, linking each old number to its new one

↑ 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: `UBTU-22-231010` and `UBTU-24-600090` raised to CAT I. Prior findings retain their historical severity in scan history.
- Linux playbooks changed this quarter, so rerun your Linux scans after the upgrade.

- Findings, comments, and custom comments recorded under **`RHEL-09-171011`** move to **`RHEL-09-271011`** automatically during the upgrade. The same applies to **`WNDF-AV-000054`**, renumbered to **`WNDF-AV-000100`** in Q3.
- Systems running Exchange 2016 or 2019 Edge will report a new CAT I finding from the sunset requirement; disposition per your organization's migration plan.

Support

For questions or issues related to this release:

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