

UNCLASSIFIED



MICROSOFT WINDOWS 11 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 1

24 July 2024

Developed by DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION	1
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions	1
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer	3
2. ASSESSMENT CONSIDERATIONS	4
2.1 Security Assessment Information	4
2.2 Group Policy Administrator Template Additions	4
3. GENERAL SECURITY REQUIREMENTS.....	5
3.1 Windows 11 Enterprise Edition	5
3.2 Hardware and Firmware	5
3.3 Virtualization-Based Security Hypervisor Code Integrity	6
3.4 Virtual Desktop Implementations.....	6
3.5 Windows Applications.....	6
3.6 Windows as a Service	7
3.7 Cortana	8

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Windows 11 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs, such as the Windows Defender Antivirus STIG, Microsoft Edge STIG, MS OneDrive STIG, and appropriate operating system STIGs.

This Microsoft Windows 11 Enterprise Security Requirements Guide (SRG) provides the technical security policies and requirements for applying security concepts to systems.

The requirements discussed in this document are applicable to Windows 11 Enterprise. The majority will also apply to Windows 11 Professional; however, domain-joined systems have several requirements that can only be implemented with the Enterprise edition.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA

implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The Windows Operating Systems STIG Overview, available on Cyber Exchange, is a summary-level document for the various Windows Operating System STIGs. Additional information can be found there.

2.2 Group Policy Administrator Template Additions

Some of the requirements in this STIG depend on the use of additional group policy administrative templates that are not included with Windows by default. These administrative template files (.admx and .adml file types) must be copied to the appropriate location in the Windows directory to make the settings they provide visible in group policy tools.

This includes settings under MS Security Guide and MSS (Legacy). The MSS settings have previously been made available through an update of the Windows security options file (sceregl.inf). This required a change in permissions to that file, which is typically controlled by the system. A custom template was developed to avoid this. The custom template files (MSS-Legacy and SecGuide) are provided in the Templates directory of the STIG package. The .admx files must be copied to the \Windows\PolicyDefinitions\ directory. The .adml files must be copied to the \Windows\PolicyDefinitions\en-US\ directory.

3. GENERAL SECURITY REQUIREMENTS

3.1 Windows 11 Enterprise Edition

Hardware that supports TPM 2.0 will be needed to install or run Windows 11. Organizations must ensure TPM 2.0 is ready to use.

UEFI firmware is required to support Secure Boot. Many current systems have UEFI firmware; however, it may have been configured to operate in legacy BIOS mode with earlier Windows versions. Changing this will require a complete reinstallation of the operating system instead of an in-place upgrade.

Credential Guard will be required in Windows 11 Enterprise Edition. Domain-joined systems will need to use this edition to meet the related requirements.

The Windows 11 processor should be 1 gigahertz (GHz) or faster with two or more cores on a compatible 64-bit processor or System on a Chip (SoC).

<https://docs.microsoft.com/en-us/windows-hardware/design/minimum/windows-processor-requirements>

The system CPU must support virtualization. Again, most current CPUs have this capability; however, it may need to be enabled in the firmware.

<https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard>

3.2 Hardware and Firmware

The virtualization-based security features have hardware and firmware requirements as well as Windows 11 Enterprise Edition.

UEFI firmware is required to support Secure Boot. Many current systems have UEFI firmware; however, it may have been configured to operate in legacy BIOS mode with earlier Windows versions. Changing this will require a complete reinstallation of the operating system instead of an in-place upgrade.

Also, the system CPU must support virtualization. Again, most current CPUs have this capability; however, it may need to be enabled in the firmware.

A Microsoft article on Credential Guard, including system requirement details, can be found at the following link:

<https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard>

3.3 Virtualization-Based Security Hypervisor Code Integrity

Windows 11 Virtualization Based Security (VBS) Device Guard feature, known as Hypervisor Code Integrity (HVCI), may cause major functional issues when running older or non-compliant drivers. The HVCI service in Windows 11 determines whether code executing in kernel mode is securely designed and trustworthy. It offers zero-day and vulnerability exploit protection capabilities by ensuring that all software running in kernel mode, including drivers, securely allocate memory and operate as they are intended.

When developing or testing Windows 11 drivers, it is critical that the drivers are HVCI-compliant. Hardware drivers must support HVCI if the Device Guard HVCI feature is enabled on the target system. When HVCI is enforced, functional issues have been observed on hardware running non-HVCI-compliant drivers. The issues are commonly encountered with kernel mode device drivers, such as video adapters, third-party disk encryption software, anti-virus/anti-malware software, or traditional BIOS or other firmware. The HVCI conflicts range from minor (video resolution issues) to major (boot failures or Blue Screen). Confirm with the hardware vendor that their drivers support HVCI and are tested before implementing the Windows 11 Device Guard HVCI feature.

3.4 Virtual Desktop Implementations

Virtualization-based security, including Credential Guard, must be implemented in Virtual Desktop Implementations (VDIs) supporting requirements including a TPM v2.0, UEFI with Secure Boot, and the capability to run the Hyper-V feature within the virtual desktop.

The STIG requirements refer to non-persistent and persistent desktops for mitigations. Persistence refers to the state of the desktop, not the user data. Non-persistent desktops are deleted or refreshed at user logoff. This prevents the accumulation of credential artifacts in the system. Persistent desktops are not deleted or refreshed at user logoff allowing for re-use. The STIG currently allows these requirements to be not applicable where the virtual desktop instance is deleted or refreshed upon logoff.

3.5 Windows Applications

Windows 11 includes a number of universal applications provisioned and installed by default on the system. These apps may change over time and with different versions of Windows 11. This includes the Store app for downloading additional apps. Access to the Windows Store may be turned off through a group policy setting to prevent access to Windows apps. The policy, "Turn off the Store application" is located at Computer Configuration >> Administrative Templates >> Windows Components >> Store.

The use of allowlisting is an effective method to control the universal apps allowed to run. This will also prevent unapproved apps that are downloaded from the Store from running.

Care must be taken with the allowlisting of universal apps. Several system-related items such as the Start Menu are also in the form of appx packages. The built-in program, AppLocker, can scan a system and automatically create rules for existing apps such as the system apps.

It is recommended any pre-provisioned apps the organization does not want on a system be removed before users log on to the system. This will prevent these apps from being installed in the user's profile when they first log on. The Store app may also be removed with this method. If the default apps are installed in a user profile, there may not be an uninstall option for the app in the Apps & Features settings. PowerShell can be used to remove them.

To remove preprovisioned apps from a system:

- Run **Windows PowerShell** as an administrator.
- Enter **Get-AppxProvisionedPackage -online**.
- Make note of the **PackageName**.
 - e.g., Microsoft.MicrosoftSolitaireCollection_3.1.6103.0_neutral_~_8wekyb3d8bbwe
- Enter **Remove-AppxProvisionedPackage -online -packagename [packagename]**.
 - Substitute **[packagename]** with the name noted from the previous step.

To obtain a list of apps installed in user profiles:

- Run **Windows PowerShell** as an administrator.
- Enter **Get-AppxPackage -User [username]**, substituting **[username]** with the user account.

To remove apps from a user profile:

- Log on with the account from which the apps are to be removed.
- Run **Windows PowerShell**.
- Enter **Get-AppxPackage** to obtain a list of app packages for the user, if needed.
Note: The list will include system apps as well. Ensure to only uninstall actual user apps.
- Make note of the **PackageFullName** of apps to be removed.
 - e.g., Microsoft.MicrosoftSolitaireCollection_3.1.6103.0_neutral_~_8wekyb3d8bbwe
- Enter **Remove-AppxPackage -Package [PackageFullName]**, substituting **[PackageFullName]** with the name noted from the previous step.

3.6 Windows as a Service

Microsoft has implemented a new model for updating Windows, referred to Windows as a Service (WaaS). New features and non-security-related updates will be applied to the system on an ongoing basis.

New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 months. The initial release of a feature update is the Semi-Annual Channel (Pilot), previously referred to as the Current Branch (CB). Approximately four months after a new release it is declared Semi-Annual Channel (Broad), previously referred to as the Current Branch for Business (CBB). Only two active versions will be supported with updates at any given time (with some overlap during the period the latest version is declared Semi-Annual Channel [Broad] and support is ending for the oldest version.) This will require organizations to test and maintain systems at a supported level in an ongoing basis.

The Windows 11 STIG may be updated as new features are added based on Microsoft's WaaS model. The STIG may include requirements that are applicable to the most recent version. Settings may also vary between versions as Microsoft updates policy names or selection options.

A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates. Systems using an LTSC version may not be able to meet all requirements of the STIG as new features are added, which organizations will need to address.

3.7 Cortana

Cortana is Microsoft's personal assistant built into Windows 11. Cortana can collect various information about a user such as preferences, location, and history. Cortana requires a Microsoft account to store this information in the cloud. If an organization chooses not to allow Cortana, it can be disabled using the following group policy setting:

Computer Configuration >> Administrative Templates >> Windows Components >> Search >> "Allow Cortana"