



WINDOWS SERVER 2016
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

Version 1, Release 12

17 June 2020

Developed by DISA for the DoD

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 DISA of any non-Federal 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 Document Revisions 2
1.6 Other Considerations 2
1.7 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Security Assessment Information 4
2.2 Windows Server 2016 Installation Options 4
2.3 Group Policy Administrative Template Additions 4

3. GENERAL SECURITY REQUIREMENTS 5

3.1 Hardware and Firmware 5
3.2 Virtualization-Based Security Hypervisor Code Integrity 5

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Windows Server 2016 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed by DoD Consensus as well as Windows security guidance by Microsoft Corporation. This document is meant for use in conjunction with other applicable STIGs including such topics as Active Directory Domain, Active Directory Forest, and Domain Name Service (DNS).

The Windows Server 2016 STIG includes requirements for both domain controllers and member servers/standalone systems. Requirements specific to domain controllers have "DC" as the second component of the STIG IDs. Requirements specific to member servers have "MS" as the second component of the STIG IDs. All other requirements apply to all systems.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (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, 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 need to 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

	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 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 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.

1.6 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 Authorizing Official. 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 Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7 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). DoD Authorizing Officials (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 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) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

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

2.2 Windows Server 2016 Installation Options

Windows Server 2016 has two main installation options. The server core installation is the default option. This option provides a reduced footprint and attack surface in which the standard graphical user interfaces (GUIs) are not available, with a few exceptions. Interacting with the system when logged on locally is done through a command line environment. Server core installations may also be managed remotely from another system with many of the standard GUIs. Not all server roles are supported in Server core installations.

The Windows Server 2016 (Desktop Experience) installation option provides the standard interfaces for interacting with the system. This may include binaries not specifically required for the system to function and increases the attack surface.

A new installation type is Nano Server. Nano Server is reduced even further than server core. It is not created from the standard installation media. Nano Servers are created with PowerShell to include specific components required for the server.

2.3 Group Policy Administrative 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 had previously been made available through an update of the Windows security options file (sceregvl.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 Hardware and Firmware

The virtualization-based security features, including Credential Guard, have specific hardware and firmware requirements.

Unified Extensible Firmware Interface (UEFI) is required to support Secure Boot. Current systems may have UEFI; however, it may have been configured to operate in legacy Basic Input/Output System (BIOS) mode with earlier Windows versions. Changing this will require a complete reinstallation of the operating system instead of an in-place upgrade.

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

A Trusted Platform Module (TPM) is required to store the keys used by Credential Guard. Credential Guard can function without a TPM; however, the keys are stored in a less secure method in software.

A Microsoft TechNet article on Credential Guard, including system requirement details, can be found at the following link: https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard

3.2 Virtualization-Based Security Hypervisor Code Integrity

The Windows Virtualization-Based Security (VBS) Device Guard feature known as Hypervisor Code Integrity (HVCI) may cause major functional issues when running older or noncompliant drivers. The HVCI service in Windows 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 allocates memory and operates as intended.

When developing or testing Windows 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 older, as well as recent, 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 your hardware vendor that its drivers support HVCI and are tested before implementing the Windows Device Guard HVCI feature.