

UNCLASSIFIED



**MICROSOFT WINDOWS DEFENDER FIREWALL  
WITH ADVANCED SECURITY  
SECURITY TECHNICAL IMPLEMENTATION GUIDE  
(STIG) OVERVIEW**

**Version 2, Release 2**

**09 November 2023**

**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**

	<b>Page</b>
<b>1. INTRODUCTION .....</b>	<b>1</b>
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
<b>2. ASSESSMENT CONSIDERATIONS .....</b>	<b>4</b>
2.1 Configuration and Verification .....	4
2.2 Windows Firewall Rules .....	4

**LIST OF TABLES**

	<b>Page</b>
Table 1-1: Vulnerability Severity Category Code Definitions .....	2

## 1. INTRODUCTION

### 1.1 Executive Summary

The Security Technical Implementation Guide (STIG) for Microsoft Windows Defender Firewall with Advanced Security is published as a tool to improve the security of Department of Defense (DOD) information systems.

Starting with Windows Vista and Windows Server 2008, Microsoft included the Windows Defender Firewall with Advanced Security, which provides significant enhancements over the previous Windows Firewall. This document provides guidance specifically for Windows Defender Firewall with Advanced Security for systems that are not capable of using an approved ESS Host Intrusion Prevention (HIP) firewall.

This document is meant for use in conjunction with the appropriate operating system (OS) STIGs.

### 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**

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

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto: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 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.

## 1.7 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). 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](mailto: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) (<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 Configuration and Verification

The use of Local or Group policies is the preferred method of configuring requirements on Windows systems where applicable. The policy settings are provided in the Fix Text of the requirements. In an Active Directory environment, Group and Local policies must be applied appropriately to ensure the effective settings support STIG requirements.

The verification of many of these requirements is done in the registry with the specifics provided in the Check Content section. This aligns with verification methods used by automated tools for these requirements.

There may be some variations between Windows versions in settings labels and configuration names that are not specifically addressed if the differences are minor.

### 2.2 Windows Firewall Rules

The Windows Defender Firewall with Advanced Security has default rules to allow or deny connections to systems. These rules are automatically adjusted on Windows Servers as roles are added or removed to allow the necessary ports, protocols, etc. Rules for specific applications will need to be managed by the sites.