

UNCLASSIFIED



MCAFEE APPLICATION CONTROL 8.x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 5

26 July 2019

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 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	2
1.4 STIG Distribution.....	2
1.5 Document Revisions	2
1.6 Other Considerations.....	2
1.7 Product Approval Disclaimer.....	3
2. ASSESSMENT CONSIDERATION	4
2.1 SECURITY ASSESSMENT INFORMATION.....	4
2.1.1 Performing an Assessment	4

LIST OF TABLES

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

1. INTRODUCTION

1.1 Executive Summary

This McAfee Application Control Security Technical Implementation Guide (STIG) is intended to provide guidance for McAfee Application Control on DoD workstation endpoints. McAfee Application Control is a portion of the McAfee Application/Change Control product. This STIG does not include guidance for servers or for McAfee Change Control. This STIG is only applicable in a Host Based Security System (HBSS) managed environment.

The current baseline version of McAfee Application Control is 8 and above. This STIG reflects requirements as they relate to McAfee Application Control 8 and above.

McAfee Application Control is a McAfee ePolicy Orchestrator (ePO) managed software and is capable of blocking unauthorized applications and code on servers, corporate desktops, and fixed-function devices using centrally managed application whitelist(s). McAfee Application Control's dynamic trust model and security features block advanced persistent threats (APTs) without requiring signature updates or list management.

McAfee Application Control configuration for a centrally managed client is accomplished via ePO policies deployed to the client. While the McAfee Application Control can be configured by the Command Line Interface (CLI), the CLI is required to be disabled on a centrally managed McAfee Application Control installation.

The McAfee Application Control STIG provides security policy and configuration requirements. The HBSS STIG Overview provides an overview of all McAfee HBSS products and services. Both documents can be referenced on the Cyber Exchange website at <https://cyber.mil> or <https://public.cyber.mil>

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 CONSIDERATION

2.1 SECURITY ASSESSMENT INFORMATION

2.1.1 Performing an Assessment

To be in compliance with this STIG and perform an assessment of the McAfee Application Control module in the McAfee ePO server, an organization must have a documented, organization-specific, written policy for the McAfee Application Control.

The written policy will be used as a basis for determining compliance with several of the McAfee Application Control requirements in the STIG, such as organization-specific variables for the application whitelisting, procedures for how whitelisted applications are deemed to be allowed, and identifying the frequency of the review of whitelisted applications.

The written policy will be initially approved by and maintained by the Information System Security Officer/Information System Security Manager/Authorizing Official (ISSO/ISSM/AO) at that location.

The written policy must be under a formalized change control process to ensure changes to the written policy are made in a controlled manner. Changes must undergo a formal review process requiring signed acceptance by the ISSO/ISSM/AO at that location.

If the organization has a formal Change Advisory Board (CAB) or Configuration Control Board (CCB), the McAfee Application Control written policy must be under its oversight.

As the required method of managing the McAfee Application Control is through the ePO server, most of the review is performed in the ePO console.

When being managed by the ePO server, a McAfee Application Control/Solidcore client's Command Line Interface (CLI) will be in lockdown mode automatically by default.

Because the CLI can be recovered by a System Administrator, the written policy requirements for the CLI password management has been included in the STIG. This written policy must be applied even though the CLI is in lockdown in production.

Under a CLI recovered condition, the endpoint is unable to receive ePO pushed policies and must be returned to lockdown after troubleshooting has been accomplished.