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

**Version 3, Release 1**

**24 July 2024**

**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 Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

# TABLE OF CONTENTS

Page

## LIST OF TABLES

# 1. INTRODUCTION

## 1.1 Executive Summary

This Trellix Application Control Security Technical Implementation Guide (STIG) is intended to provide guidance for Trellix Application Control on DOD workstation endpoints. Trellix Application Control is a portion of the Trellix Application/Change Control product. This STIG does not include guidance for servers or for Trellix Change Control. This STIG is only applicable in an Endpoint Security Solutions (ESS) managed environment.

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

Trellix Application Control is a Trellix 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 allowlist(s). Trellix Application Control's dynamic trust model and security features block advanced persistent threats (APTs) without requiring signature updates or list management.

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

The Trellix Application Control STIG provides security policy and configuration requirements. The ESS STIG Overview provides an overview of all Trellix ESS 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

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 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 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. 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 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 Trellix Application Control module in the Trellix ePO server, an organization must have a documented, organization-specific, written policy for the Trellix Application Control.

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

As the required method of managing the Trellix 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 Trellix 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.