ARISTA MULTILAYER SWITCH (MLS)
DCS-7000 SERIES
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

24 July 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

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Arista Multilayer Switch (MLS) DCS-7000 Series Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Arista MLS DCS-7000 Series devices.

The Arista MLS DCS-7000 Series STIG is a package of three (3) STIGs for configuring Arista MLS DCS-7000 Series devices according to the configuration and purpose of the device. The following are the three STIGs included as part of the Arista MLS DCS-7000 Series STIG package:

- Arista MLS DCS-7000 Series Network Device Management (NDM) STIG
- Arista MLS DCS-7000 Series Layer 2 Switch (L2S) STIG
- Arista MLS DCS-7000 Series Router (RTR) STIG

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 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 For Official Use Only (FOUO) will be available for those 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 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.

1.8 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). 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 Arista MLS DCS-7000 Series switches incorporate both Layer 2 and Layer 3 capabilities. Because of the flexible nature of the Arista multilayer switches, these products may be used in several different configurations for multiple purposes. Therefore, it is critical to assess Arista MLS DCS-7000 Series switches using all three STIGs provided in the package to prevent gaps in security. The Arista MLS DCS-7000 Series Network Device Management (NDM) STIG, Arista MLS DCS-7000 Series Layer 2 Switch (L2S) STIG, and Arista MLS DCS-7000 Series Router (RTR) STIG contain the specific configuration guidance for each of these functional areas.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Overview

The Arista MLS DCS-7000 Series multilayer switches have broad capabilities that enable these devices designed primarily to be used as data center switches, to be used for other purposes. Within the data center, the multilayer switch may be used as a spine switch or leaf switch. Outside the data center, these correspond to distribution switches and access switches. Because of the high bandwidth, these switches may also be used as core communications switches or perimeter routing switches. In specific configurations, some requirements may be applicable that would otherwise be not applicable.

3.2 Access Switch

When the Arista MLS DCS-7000 Series switch is used as an access device, providing connectivity to end user devices, the requirements for access control must be enabled. These requirements have text within the check procedure stating, "This requirement only applies to access switches required to employ 802.1x."

3.3 Boundary Router

When the Arista MLS DCS-7000 Series switch is used as a boundary device, routing external-facing network traffic, the requirements for boundary routing must be enabled. These requirements have text within the check procedure stating, “This requirement only applies to external-facing interfaces of a network edge router”.

3.4 DODIN Enclave Router

When the Arista MLS DCS-7000 Series switch is used within the DoD Information Network (DODIN) enclave, the requirements pertaining to enclave routing must be enabled. These requirements have text within the check procedure stating, “This requirement only applies to DODIN enclaves”.

4. GENERAL SECURITY REQUIREMENTS

4.1 Overview

The implementation of the Arista MLS DCS-7000 Series STIGs occurs in three (3) parts. The Arista MLS DCS-7000 Series NDM STIG is used to configure the management plane of the Arista MLS DCS-7000 Series network switch. The Arista MLS DCS-7000 Series L2S and RTR STIGs are used to configure the Layer 2 and Layer 3 capabilities within the network switch.

4.2 Arista MLS DCS-7000 Series Device Management Configuration

The Arista MLS DCS-7000 Series NDM STIG is used to configure the management plane of the Arista MLS DCS-7000 Series network switch. This covers the requirements for administrator access, event logging, and other management configuration settings.

4.3 Arista MLS DCS-7000 Series Layer 2 Switch Configuration

The Arista MLS DCS-7000 Series L2S STIG is used to configure the Layer 2 capabilities of the data plane. This includes requirements for implementing 802.1x, spanning tree protocol, and other Layer 2 configuration settings.

4.4 Arista MLS DCS-7000 Series Router Configuration

The Arista MLS DCS-7000 Series RTR STIG is used to configure Layer 3 capabilities of the data plane. This provides for multicast, routing protocols, access lists, and other Layer 3 configuration settings.