

UNCLASSIFIED



XYLOK SECURITY SUITE 20.X SECURITY TECHNICAL IMPLEMENTATION GUIDE OVERVIEW

Version 1, Release 1

10 December 2024

Developed by Xylok and 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

	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 – External Identity and Access Management.....	4
2.2 Security Assessment Information – Central Log Server.....	4
2.3 Security Assessment Information – Django.....	4
2.4 Security Assessment Information – Debian.....	4
3. ARCHITECTURE	5
4. GENERAL SECURITY REQUIREMENTS.....	6

LIST OF TABLES

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

LIST OF FIGURES

	Page
Figure 3-1: Xylok Architecture	5

1. INTRODUCTION

1.1 Executive Summary

The Xylok Security Suite 20.x Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with the appropriate operating system STIGs.

This STIG applies to the Xylok Security Suite and assumes the product is installed and configured in accordance with the documented installation instructions provided by Xylok. This STIG also assumes delegation of certain security control implementation to external, integrated enterprise systems including a central identity and access management system, central logging management system, and others as noted in this document.

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 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. 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.
- DODIN Approved Products List (APL) (<https://aplists.disa.mil/processAPList.action>) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

This STIG is not intended to provide technical guidance for all portions of Xylok. Xylok is a complex software system, and this STIG is applicable to only a subset of the potential set of components available for use in and with Xylok, all applicable subcomponents are part of default installation per the installation instructions provided with the platform.

2.1 Security Assessment Information – External Identity and Access Management

This STIG delegates certain security controls to an external Identity and Access Management system; delegated controls are out of scope of this STIG. Security controls in this STIG ensure the correct integration of this external system but thereafter rely on the security capabilities of this system.

Xylok allows the use of a number of supported providers including Active Directory, LDAP, and others. This STIG was tested and validated using Active Directory.

2.2 Security Assessment Information – Central Log Server

Integrating a central log server for managing audit records within the Xylok Security Suite is required in this STIG. By providing centralized logging, real-time analysis, and automated alerting, a central log server allows Xylok to maintain a robust security posture and effectively respond to potential threats, ultimately contributing to the organization's overall security strategy.

2.3 Security Assessment Information – Django

Xylok Security Suite leverages Django to manage its security operations by utilizing its authentication system for role-based access control, creating APIs for security tasks via Django REST Framework (DRF) and building dynamic dashboards analytics. Django's middleware is employed to implement a consent banner for privacy compliance, while its admin panel aids in managing backend configurations and user permissions.

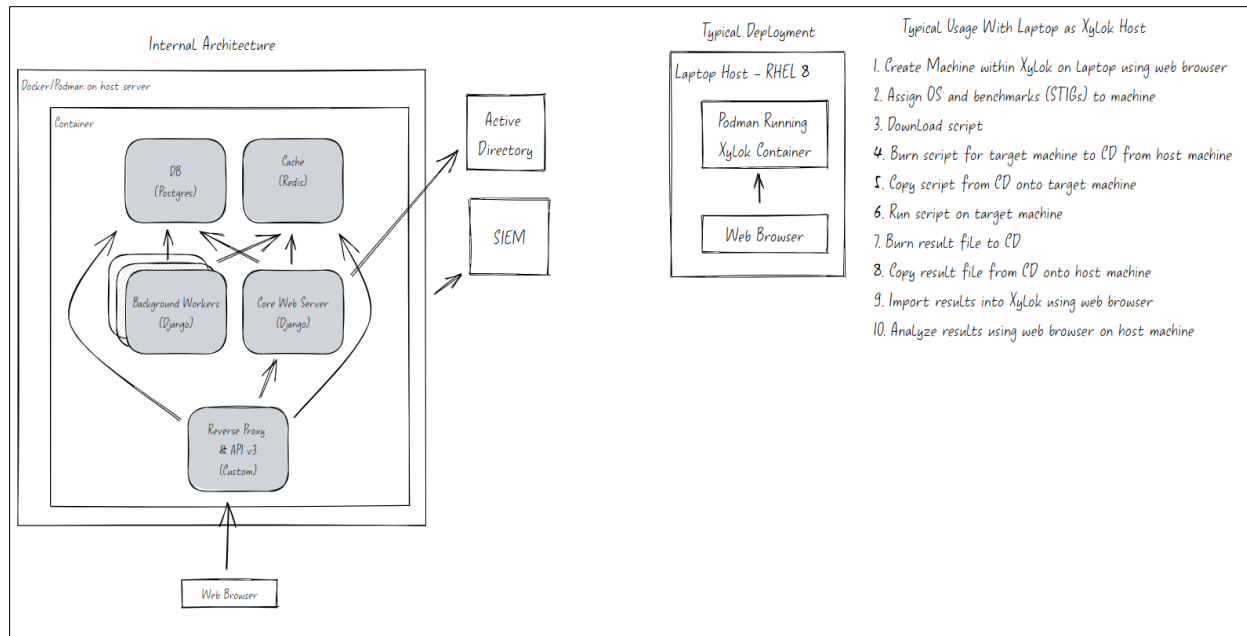
2.4 Security Assessment Information – Debian

Xylok Security Suite uses a Debian container to streamline its operations, leveraging the containerized environment for consistency and scalability. Within this container, Xylok taps into the underlying operating system's urandom functionality to generate secure, random session IDs. By utilizing urandom, Xylok ensures that session IDs are cryptographically secure, reducing the risk of predictability in session management and enhancing the overall security of the platform.

3. ARCHITECTURE

Xylok Security Suite's architecture is designed for scalability, modularity, and security. The core backend is built using Django, which provides a foundation for API management and web services, while leveraging containers (like Debian) for a consistent and isolated runtime environment. Xylok integrates with external security tools and APIs, with each microservice communicating over secure channels. Additionally, it incorporates robust logging, monitoring, and real-time alerting mechanisms, ensuring comprehensive oversight and rapid response to security incidents.

Figure 3-1: Xylok Architecture



4. GENERAL SECURITY REQUIREMENTS

Xylok relies on Docker or Podman for its operation. All updates to the container images must be done via a Xylok-supplied install script. Every new build of a Xylok container includes a container image based on the latest revision of Python.