

UNCLASSIFIED



TANIUM 6.5 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

28 October 2016

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	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	4
2.1.1 NIST SP800-53 Requirements	4
2.1.2 Tanium 6.5 Best Practices	4
2.1.3 Tanium Configuration for CAC Authentication.....	4
2.1.4 Tanium Implemented Controls Specific to DoD and Federal Systems	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS	5
3.1 Tanium 6.5 Functionality	5
3.2 Tanium 6.5 Infrastructure.....	6
4. GENERAL SECURITY REQUIREMENTS	7
4.1 Security Posture of Tanium Platform.....	7

LIST OF TABLES

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

1. INTRODUCTION

1.1 Executive Summary

This Tanium 6.5 Security Technical Implementation Guide (STIG) is intended to provide security guidelines for the protection of the Tanium Application and its components, including but not limited to the Tanium Application, Tanium Console, Tanium Module Server, Tanium Clients, and Tanium SQL Database.

Tanium 6.5 is a scalable Endpoint Security and Management system. Its foundation is the Tanium Core. Tanium Core includes basic asset inventory, control and utilization monitoring capabilities, and connectors for integrating with third-party systems.

Tanium uses a linear peer-to-peer architecture specifically designed for fault tolerance, transient endpoints, and the global Wide Area Network (WAN) segments. It is not a typical peer-to-peer application; only other Tanium endpoints can communicate over the peer-to-peer architecture. The clients communicate with each other over a specific Transmission Control Protocol (TCP) port.

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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is <http://iase.disa.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 CONSIDERATIONS

2.1 Security Assessment Information

2.1.1 NIST SP800-53 Requirements

Requirements used in this STIG have been built upon applicable baseline technical NIST SP 800-53 requirements and security best practice requirements as are included in the Application Security Requirement Guide (SRG).

CNSSI 1253 defines the required controls for DoD systems based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.1.2 Tanium 6.5 Best Practices

The Tanium 6.5 Best Practices have been incorporated into this STIG. These published Best Practices can be located on the Tanium Knowledge Base website at:

https://kb.tanium.com/Knowledge_Base

2.1.3 Tanium Configuration for CAC Authentication

To implement Common Access Card (CAC) authentication for access to the Tanium Server console, follow the procedures found on the vendor site at the following URL:

https://kb.tanium.com/Smart_Card_Authentication

2.1.4 Tanium Implemented Controls Specific to DoD and Federal Systems

The Tanium Server's web-based Console must be configured to allow access only via CAC smartcard authentication. It also requires the syncing of the Console user accounts with Active Directory (AD) so that roles and delegation of functions can be segregated by AD security groups. These AD security groups sync to Tanium as user roles. The CAC authentication will use the AD account for access to the Console and will provide the Tanium Role as is identified by the respective AD security group.

The actual syncing of the Tanium Console to the AD is configured in the Module Server via the Connection Manager.

The configuration is a multi-step process implementing multiple registry keys on the Tanium Server designed to enforce the CAC authentication requirement.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Tanium 6.5 Functionality

Tanium Application Server manages client registrations and provides clients with environmental perspective. It signs sensors (questions) and packages (actions) and performs other security configuration tasks.

Sensors are scripts written in a variety of non-proprietary languages, customized for any ad-hoc questions, and capture the answers globally across OS platforms. Tanium includes more than 800 core sensors out of the box. Most sensors contain multiple data points, and many can be combined, filtered, sorted, and parameterized from a simple natural language user interface (UI), allowing the System Administrator to ask an infinite number of questions of the clients without ever having to write even a single script.

Packages are the actions that you want to take on clients using Tanium. The packages are composed of commands that you want to issue, similar to sitting at the command line of the machine, and any files that need to be distributed for those commands to run, including tools, patches, application updates, new software, or service packs.

Tanium Console is a web-based application used to easily ask questions, display answers, and take actions. Using the SOAP API, the Tanium Console's full functionality is available to any other system that can issue a SOAP request and consume the response. The query and action events deployed through the SOAP API provide the same role-based restrictions as users working directly from the console, so visibility and management can be carefully controlled even when integrated into external systems.

Tanium Client is a light-weight and optimized agent deployed by the Tanium Application Server to each endpoint, making the endpoint a client. The client initiates traffic between itself, the Tanium Application Server, and other peer clients and exchanges and answers questions. It also distributes packages that have a valid signature.

Tanium Zone Server is an optional server that allows roaming devices to remain in contact with the Tanium Application Server. It is typically installed to one or more devices in a DMZ and can answer questions and perform actions as if it were connected to the network.

Tanium IOC Funnel allows security analysts to import Indicators of Compromise (IOC) easily. Tanium IOC Funnel can combine the IOCs into one set of questions, minimizing the overhead of the IOC scans. It allows Tanium to evaluate multiple IOCs in a single scan, which can accelerate incident response.

Tanium Connection Manager provides a flexible and powerful framework to automate the integration of Tanium with other systems within the enterprise, as well as interactions with other APIs and services. Through a simple interface that requires no scripting, administrators are able to "string together" endpoint data surfaced through simple saved questions with one or more connections to back-end systems, data processing tasks, or other services, such as Security

Information and Event Management (SIEM) (Splunk, HP ArcSight, and IBM QRadar); discover and compare new behavioral data to threat feeds; drive new data to big data analytics tools; or share audit and inventory data with Configuration Management Databases (CMDBs).

3.2 Tanium 6.5 Infrastructure

Tanium is not built on a hierarchical server infrastructure to provide data collection, aggregation, and distribution functionality. Instead, Tanium uses a linear peer-to-peer architecture specifically designed for fault tolerance, transient endpoints, and the global WAN segments. It is not a typical peer-to-peer application; only other Tanium endpoints can communicate over the peer-to-peer architecture. The clients communicate with each other over a specific TCP port.

The following highlights these key architectural differences:

- Traditional Communications Flow
 - Server propagates request to all relay servers
 - Relay server collects individual responses from its clients
 - Relay server sends series of individual responses back to server
- Tanium Communications Flow
 - Tanium Server contacts a few clients
 - Client contacts peer client and passes aggregated response over LAN
 - Last client sends final aggregated response to server

4. GENERAL SECURITY REQUIREMENTS

4.1 Security Posture of Tanium Platform

Since every implementation of Tanium will have its own nuances, this STIG is not an all-encompassing STIG intended to provide complete end-to-end guidance for the Tanium architecture but is intended to secure the areas where compromise could occur.

The security posture of the Tanium components requires the full configuration of all platform STIGs, including the OS STIG, browser, SQL database, antivirus, web, and any other feature installed on any of the components for which a STIG exists.

This STIG does not provide operational guidance for the multiple Tanium functionalities. For instance, this STIG does not outline how to package an update and deploy to the clients. It will, however, provide specific configuration guidance if a function of Tanium could impact the security posture of the Tanium platform. For instance, deploying the Tanium Client Agent via the Client Deployment Tool has the ability to use psexec. The STIG prohibits the use of psexec.

The STIG is one consolidated STIG, although the requirements might span across different Tanium servers, the clients, or the SQL database server. Many of the client requirements can be accomplished on the Tanium server itself, via the console, by asking questions of the clients.