

UNCLASSIFIED



# **IVANTI SENTRY 9.x SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW**

**24 October 2024**

**Developed by Ivanti 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
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions .....	1
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting .....	2
1.6 Document Revisions .....	2
1.7 Other Considerations .....	2
1.8 Product Approval Disclaimer .....	3
<b>2. ASSESSMENT CONSIDERATIONS .....</b>	<b>4</b>
2.1 Security Assessment Information .....	4
<b>3. IVANTI SENTRY SECURITY AND CONFIGURATION INFORMATION .....</b>	<b>5</b>
3.1 IvantiSentry Architecture.....	5
3.1.1 Device First Attempt to Access the ActiveSync Server.....	5
3.2 Ivanti Sentry Software Components .....	6
3.3 Ivanti Sentry Required Firewall Ports .....	6

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions .....	2
Table 3-1: Ivanti Sentry Components .....	6
Table 3-2: Required Ports and Services.....	6

## LIST OF FIGURES

	<b>Page</b>
Figure 3-1: Ivanti High-Level Architecture.....	5
Figure 3-2: Ivanti Detailed Architecture .....	6

## 1. INTRODUCTION

### 1.1 Executive Summary

The Ivanti Sentry 9.x Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This STIG is based on security controls found in both the Application Layer Gateway (ALG) Security Requirements Guide (SRG) and the Network Device Management (NDM) SRG. This document is meant for use in conjunction with the Ivanti Endpoint Manager Mobile (EPMM) Server STIG.

This STIG assumes additional network services and components are available to support the Sentry deployment. See section 2 for more information.

### 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**

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> 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 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 Controlled Unclassified Information (CUI) will be available for 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](mailto: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](mailto: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 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.

## 1.8 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). 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](mailto: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 CONSIDERATIONS

### 2.1 Security Assessment Information

This STIG makes the following assumptions:

- Backend applications are responsible for implementing authentication controls for the connected mobile device or mobile device user before access to the application is granted.
- Backend applications are responsible for presenting the DOD warning banner to mobile device users before access to the application is granted.
- It is the responsibility of other network components to perform traffic inspection of inbound and outbound traffic from Sentry.

### 3. IVANTI SENTRY SECURITY AND CONFIGURATION INFORMATION

#### 3.1 Ivanti Sentry Architecture

Ivanti Sentry is a part of an Ivanti deployment that serves as an intelligent gatekeeper to an organization's ActiveSync server, such as a Microsoft Exchange Server, or with a backend resource such as a SharePoint server, or it can be configured as a Kerberos Key Distribution Center Proxy (KKDCP) server. Sentry obtains configuration and device information from an Ivanti EPMM.

The figure below illustrates the interaction between Standalone Sentry, UEM, and the device when the device first attempts to access the ActiveSync server.

**Figure 3-1: Ivanti High-Level Architecture<sup>1</sup>**

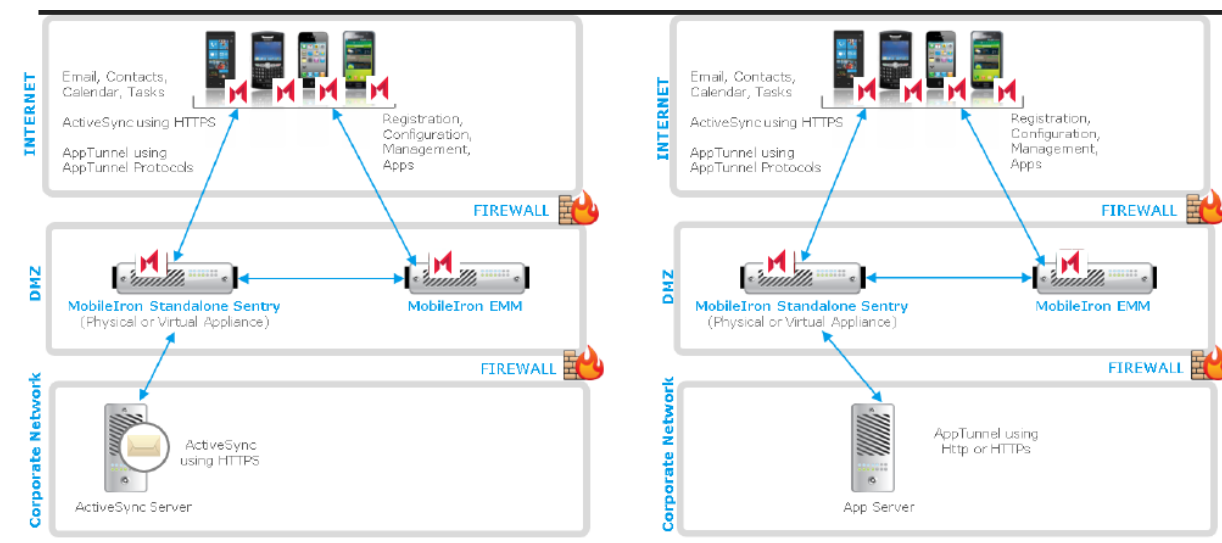


##### 3.1.1 Device First Attempt to Access the ActiveSync Server

1. Device attempts to access ActiveSync or other backend resource.
2. Standalone Sentry adds device to its list of devices.
3. Standalone Sentry tells UEM about the device.
4. The ActiveSync devices view on the UEM now includes the device.
5. UEM tells Standalone Sentry whether to block or allow the device based on:
  - a. The device's security policy;
  - b. Whether the maximum number of devices per mailbox has been exceeded;
  - c. Whether it has been specified to auto-block unregistered devices.
6. Sentry tells device whether it is blocked or allowed, passing ActiveSync policy if allowed.
7. If access is allowed, device applies ActiveSync policy and continues email processing.
8. If access is blocked, Standalone Sentry informs the device.

The next time a device attempts to access the ActiveSync server, the device is already in the list of devices on Standalone Sentry. Therefore, Standalone Sentry already has the information in the UEM about whether to block or allow access.

<sup>1</sup> The figure includes old product names.

Figure 3-2: Ivanti Detailed Architecture<sup>2</sup>

### 3.2 Ivanti Sentry Software Components

Table 3-1: Ivanti Sentry Components

Component	Description
Ivanti Sentry	A standalone Sentry appliance (virtual or physical) that can be deployed on premise or in Azure Cloud

### 3.3 Ivanti Sentry Required Firewall Ports

Table 3-2: Required Ports and Services

From	To	Port (TCP)	Description
Administrators	Sentry Server	22	SSH
Mobile Devices	Sentry Server	443	HTTPS
Administrators	Sentry Server	8443	HTTPS-alt

<sup>2</sup> The figure includes old product names.