

UNCLASSIFIED



OMNISSA HORIZON SECURITY TECHNICAL IMPLEMENTATION GUIDE STIG OVERVIEW

30 September 2026

Developed by Omnissa and DISA for the DoW

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	1
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer	2
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 Security Assessment Information.....	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....	6
3.1 Architecture	6

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	1
Table 2-1: Vulnerability Severity Category Code Definitions	4

LIST OF FIGURES

	Page
Figure 3-1: High-Level Architecture of Horizon Components	8

1. INTRODUCTION

1.1 Executive Summary

The OmniSSA Horizon Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of War (DoW) information systems. This document is meant for use in conjunction with other STIGs and appropriate operating system STIGs.

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 DoW 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 DoW and federal government’s computing environments can obtain the applicable STIG from the DoW 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 DoW 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.

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 DoW 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 DoW. 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 DoW architecture.

1.8 Product Approval Disclaimer

STIGs provide configurable operational security guidance for products being used by the DoW. 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 DoW Risk Management Framework (RMF). DoW 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) DoW policy and through RMF risk acceptance. Inputs into acquisition or preacquisition 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/DoW mandated standards.

2. ASSESSMENT CONSIDERATIONS

To prevent a host-level compromise from subverting Virtual Desktop Infrastructure (VDI)-specific security controls, the deployment must be built upon a pre-hardened, STIG-compliant foundation where the underlying virtualization, operating system, and directory layers (including vSphere, Windows Server, and Active Directory) strictly adhere to the mandatory baseline configurations.

Beyond the foundational infrastructure, the scope of this STIG assessment directly targets the core functional components of the Horizon ecosystem detailed below:

- **Unified Access Gateway (UAG):** Acts as a secure proxy for user connections. It prevents unauthorized external users from gaining direct access to internal Horizon Connection Servers and virtual machines.
- **Horizon Connection Server:** The central management engine of the Horizon environment. It acts as the traffic broker. It authenticates users, determines which virtual desktops or hosted applications users can access, and directs the client connection to the appropriate resource.
- **Horizon Agent:** A software service installed on the target virtual machines, physical computers, or Remote Desktop Services Host (RDSH) servers that host the actual desktops and applications. Facilitates the connection session between the client machine and the virtual operating system, rendering the desktop or application to the user.
- **Horizon Client:** The local application installed on the end-user's physical device (thin client, laptop, mobile device, or zero client) used to access their virtual environment. Communicates with the Connection Gateway to authenticate the user and decode the encrypted display protocol streams (such as Blast Extreme) to present the virtual environment.

2.1 Security Assessment Information

To evaluate the OmniSSA Horizon environment, assessors must be granted appropriate administrative visibility across multiple security enclaves. Because Horizon is a distributed architecture, the assessment cannot be performed from a single console; it requires verifying settings at the edge boundary, the brokering layer, and the guest operating system layer.

The evaluating official will require the following access levels and tools to validate compliance across the Horizon components.

Table 2-1: Vulnerability Severity Category Code Definitions

Target Component	Required Interface/Tool	Assessor Access Level Required
Horizon Connection Server	OmniSSA Horizon Console (Web User Interface [UI])	Administrators Read-Only or Auditor Role within Horizon
UAG	UAG Admin UI (Port 9443)/ Representational State Transfer Application Programming Interface (REST API)	Admin equivalent account on the UAG appliance

Target Component	Required Interface/Tool	Assessor Access Level Required
Horizon Agent & Client (Group Policy Objects [GPOs])	Active Directory Group Policy Management Console (GPMC)	Read-Only access to Domain GPOs applied to VDI Organizational Units (OUs) and Client subnets
Infrastructure/Golden Image	VMware vSphere Client/Master Virtual Machine (VM) Console	Read-Only access to vCenter; Local Administrator on the VDI Master Image

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

- **Horizon Pod:** A logical management unit delimited by a group of interconnected Connection Servers that share a common Lightweight Directory Access Protocol (LDAP) configuration database.
- **Resource Block:** A physical or logical grouping of compute, storage, and virtualization resources (typically managed by a single hypervisor manager such as VMware vCenter) that provides VDI capacity to a Horizon Pod. Using a “Pod and Block” strategy isolates failures and simplifies scaling.
- **Cloud Pod Architecture (CPA):** A feature that links multiple independent Horizon Pods across geographically separated data centers into a single federated system. This is critical for High Availability (HA) and Disaster Recovery (DR), scaling up to 250,000 concurrent sessions.
- **Instant Clones:** A provisioning technology that uses rapid virtual machine cloning to generate temporary, stateless virtual desktops on demand from a running parent VM. Clones ensure that virtual desktops are destroyed upon user logoff, wiping away any potential malware or persistent threats.
- **RDSH:** A Microsoft Windows Server role that allows multiple concurrent users to access shared desktops and applications. RDSH pools require distinct operating system-level multiuser hardening policies compared to single-user VDI desktops.
- **Display Protocol:** The software engine (such as Blast Extreme or PC-over-IP [PCoIP]) that encodes, encrypts, and transmits the guest operating system screen/pixel data to the client.
- **Global Entitlements:** A logical assignment that maps users or groups to desktop pools across different pods in a Cloud Pod Architecture (CPA). This abstract assignment ensures users are routed to their designated primary site or automatically redirected to a failover site if an outage occurs.
- **Dynamic Environment Manager (DEM):** An optional companion component used to manage personal user settings, applications, and desktop configurations dynamically. DEM replaces heavy, insecure local roaming profiles with secure, granular, policy-driven profile management.
- **OmniSSA Access:** An identity provider and workspace portal that integrates with Horizon to deliver enterprisewide single sign-on, conditional access policies, and a unified application catalog across web, Software as a Service (SaaS), and virtualized resources.
- **Blast Extreme Adaptive Transport (BEAT):** A proprietary protocol enhancement within Blast Extreme designed to dynamically adapt to varying network latency and packet loss. This ensures a secure session stream even over degraded or low-bandwidth military networks.

3.1 Architecture

Component	Description
Horizon Connection Server	The Horizon Connection Server securely brokers and connects users to the Horizon Agent that has been installed in the desktops and RDS Hosts. The Connection Server authenticates users through Active Directory and directs the request to the appropriate and entitled resource.

Component	Description
Horizon Client	The Horizon Client is installed on a client device to access a Horizon-managed system that has the Horizon Agent installed. Optionally, use a web browser as an HTML client for devices on which installing client software is not possible.
Horizon Agent	The Horizon Agent is installed on the guest operating system of the target VM or system. This agent allows the machine to be managed by Connection Servers and allows a Horizon Client to form a protocol session to the machine. Machines can be virtual desktops, RDS Hosts, or physical desktops PCs.
UAG	UAG is a virtual appliance that enables secure remote access from an external network to a variety of internal resources, including Horizon-managed resources. When providing access to internal resources, UAG can be deployed within the corporate DMZ or internal network and acts as a reverse proxy host for connections to the company's resources. UAG directs authenticated requests to the appropriate resource and discards any unauthenticated requests. It also authenticates itself using an additional layer of authentication when enabled.
Horizon Enrollment Server	The Horizon Enrollment Server delivers true Single-Sign-On (SSO) functionality by ensuring users can single-sign-on to a Horizon resource when launched from OmniSSA Access or through UAG, regardless of the authentication method.
Horizon Edge Gateway appliance	The Horizon Edge Gateway is a virtual appliance that connects a Horizon pod to Horizon Cloud Services. This is required when using Horizon Cloud control plane services such as subscription licensing.
Horizon Console	A web application that is part of the Connection Server, allowing administrators to configure the server, deploy and manage desktops, control user authentication, initiate and examine system and user events, carry out end-user support, and perform analytical activities.
Events Database	Horizon uses an external database to record information about events. A separate events database should be configured for each separate Horizon pod. An events database should be local to the Horizon pod.
RDSH Servers	Microsoft Windows servers that provide published applications and session-based remote desktops to end users.

Figure 3-1: High-Level Architecture of Horizon Components