

UNCLASSIFIED



OMNISSA WORKSPACE ONE (WS1) UEM STIG SUPPLEMENTAL PROCEDURES

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. WORKSPACE ONE UEM MDM SOFTWARE SECURITY AND CONFIGURATION INFORMATION	1
1.1 MDM Software Components	1
1.2 Workspace ONE UEM MDM Required Firewall Ports	1
1.3 OmniSSa Workspace ONE (WS1) FedRAMP vs. OmniSSa Sovereign Solution (OSS)	2
1.4 Configuration Inheritance	3
1.5 Packaging and Capabilities	3

LIST OF TABLES

	Page
Table 1-1: Workspace ONE UEM Core Components.....	1
Table 1-2: Required Ports and Services	1

1. WORKSPACE ONE UEM MDM SOFTWARE SECURITY AND CONFIGURATION INFORMATION

1.1 MDM Software Components

Table 1-1: Workspace ONE UEM Core Components

Component	Description
WS1 Intelligent Hub MDM Agent Application	WS1 Agent application installed on the mobile device to communicate with the WS1 UEM MDM Server
WS1 UEM MDM DMZ Device Services Server	WS1 UEM application server installed within DMZ for external communication to mobile devices
WS1 UEM MDM Internal Network Console Server	WS1 UEM application server installed within internal network for hosting the Administration Console
WS1 UEM SQL Database Server	WS1 UEM SQL Database installed on internal network to house MDM configuration data

1.2 Workspace ONE UEM MDM Required Firewall Ports

Table 1-2: Required Ports and Services

From	To	Port	Description
Native Mobile Device MDM Agent, WS1 Intelligent Hub MDM Agent, and User Workstation	WS1 UEM MDM DMZ Device Services Server	443 (TLS/HTTPS)	TLS/HTTPS communication between mobile device and WS1 Intelligent Hub MDM Agent application to MDM DMZ Server
WS1 Intelligent Hub Android MDM Agent	Certificate Authority (CA) Server	Customizable to Organization Requirements (Default 443 [HTTPS])	Communication from WS1 Intelligent Hub Android MDM Agent to CA Server for obtaining unique certificates
WS1 UEM MDM DMZ Device Services Server	CA Server	Customizable to Organization Requirements (Default 443 [HTTPS])	Communication from WS1 UEM MDM DMZ Device Services Server to CA Server for obtaining unique certificates
WS1 UEM MDM DMZ Device Services Server	Workspace ONE UEM SQL Database Server	1433 (TCP)	Communication from Workspace ONE UEM MDM DMZ Device Services Server to WS1 UEM SQL Database Server

From	To	Port	Description
WS1 UEM MDM DMZ Device Services Server	External Auditing Server	Customizable to Organization Requirements (Default 443 [TLS])	TLS connection via Syslog from WS1 UEM MDM DMZ Device Services Server to Enterprise External Auditing Server
WS1 UEM MDM DMZ Device Services Server	Enterprise LDAP or Directory Server	686/3269 (TLS/HTTPS)	Communication from WS1 UEM MDM DMZ Device Services Server to LDAP or Directory Server
Internal Network Workstations	WS1 UEM MDM Internal Network Console Server	443 (TLS/HTTPS)	TLS/HTTPS communication between Internal Network Workstations and WS1 UEM MDM Console Server
WS1 UEM MDM Internal Network Console Server	CA Server	Customizable to Organization Requirements (Default 443 [HTTPS])	Communication from WS1 UEM MDM Network Console Server to CA Server for obtaining unique certificates
WS1 UEM MDM Internal Network Console Server	WS1 UEM SQL Database Server	1433 (TCP)	Communication from WS1 UEM Internal Console Server to Internal WS1 UEM SQL Database Server
WS1 UEM Internal Network Console Server	External Auditing Server	Customizable to Organization Requirements (Default 443 [TLS])	TLS connection via Syslog from WS1 UEM Console Server to Enterprise External Auditing Server
WS1 UEM Internal Network Console Server	Enterprise LDAP or Directory Server	686/3269 (TLS/HTTPS)	Communication from WS1 UEM Console Server to LDAP or Directory Server

1.3 Omnissa Workspace ONE (WS1) FedRAMP vs. Omnissa Sovereign Solution (OSS)

At the time of publication, Omnissa WS1 services are available at FedRAMP High and DOD IL4. This list is continuously evolving as services are stood up and certification standards change. Refer to the latest Omnissa documentation for details.

WS1 UEM is also available via Omnissa cloud partners in the form of OSS. OSS enables an Omnissa partner to deploy core UEM cloud components as a rebranded service that is then available to end users. This Security Technical Implementation Guide (STIG) was written with both Omnissa FedRAMP and OSS in mind and is applicable to both.

1.4 Configuration Inheritance

Omnissa FedRAMP administrators and OSS administrators have the ability to make configurations mandatory, optional, or completely hidden at the global level. This may result in certain STIG configuration items not appearing at all, such as a missing tab or missing configuration sections. If a Check or Fix indicates a UI path or configuration item that is not available, the cloud service provider should be contacted to verify the enforced configuration.

1.5 Packaging and Capabilities

Omnissa WS1 FedRAMP and partner-deployed OSS services are available in multiple feature packages. The features for which the user is licensed may affect their ability to fully implement the WS1 UEM STIG and/or the endpoint device STIGs via UEM. The user should work with Omnissa or their Omnissa partner representatives to ensure the user is licensed for the features required. If a WS1 UEM STIG requirement is referencing a feature for which the user is not licensed, the requirement is Not Applicable.