

## Contents

Omnissa Workspace ONE – CLOUD .....	3
Service Description (SD) SD-1. General.....	3
SD-1.1. Editions .....	3
SD-1.1.1. Essentials .....	3
SD-1.1.1.1. Omnissa Workspace ONE Employee Essentials Edition.....	3
SD-1.1.1.2. Omnissa Workspace ONE Mobile Essentials Edition .....	4
SD-1.1.1.3. Omnissa Workspace ONE Desktop Essentials Edition.....	4
SD-1.1.1.4. Omnissa Workspace ONE UEM Essentials Edition.....	4
SD-1.1.2. Workspace ONE Standard Edition.....	6
SD-1.1.4. Workspace ONE Enterprise Edition .....	6
SD-1.2. Features Included in Editions.....	7
SD-1.2.1. Workspace ONE Hub Services.....	7
SD-1.2.2. Catalog.....	7
SD-1.2.3. People .....	7
SD-1.2.4. Notifications .....	7
SD-1.2.5. Support.....	7
SD-1.2.6. Branding.....	8
SD-1.2.7. Onboarding.....	8
SD-1.3. Access Services SD-1.3.1. Identity Broker .....	8
SD-1.3.2. Identity Provided (IdP) .....	8
SD-1.3.3. Federated SSO.....	8
SD-1.3.4. Mobile SSO .....	8
SD-1.3.5. Multifactor Authentication (MFA).....	8
SD-1.3.6. Conditional Access Control.....	8
SD-1.3.7. Workspace ONE Tunnel™ .....	9
SD-1.3.8. Workspace ONE UEM.....	9
SD-1.3.9. Workspace ONE Access .....	9
SD-1.4. Mobile Management.....	10
SD-1.4.1. Mobile Device Management .....	10
SD-1.4.2. Basic Shared Device Management.....	10

SD-1.4.4. Mobile App Management.....	10
SD-1.4.6. Mobile Email Management .....	10
SD-1.4.7. Secure Email Gateway (SEG).....	10
SD-1.4.8. Telecom Management Tools.....	10
SD-1.5. Desktop Management .....	11
SD-1.5.1. Modern Desktop Management.....	11
SD-1.5.2. Advanced Desktop Management.....	11
SD-1.5.3. Enterprise Desktop Management.....	11
SD-1.6. IT Orchestration Framework SD-1.6.1. Freestyle Orchestrator .....	11
SD-1.6.2. IT Compliance Automation Engine.....	12
SD-1.7. Reporting and Automation .....	12
SD-1.7.1. Reports.....	12
SD-1.7.2. Report Customization and Scheduling (snapshot data).....	12
SD-1.7.3. Configurable Dashboards .....	12
SD-1.7.5. Device Health and Lifecycle.....	12
SD-1.7.6. Device Health and Security.....	12
SD-1.8. Mobile Productivity Apps .....	12
SD-1.8.2. Workspace ONE Boxer.....	13
SD-1.8.4. Workspace ONE Web.....	13
SD-1.8.5. Workspace ONE Content .....	13
SD-1.8.7. Workspace ONE PIV-D Manager .....	13
SD-1.10. Remote Support for Endpoints.....	13
SD-1.10.1. Workspace ONE Assist for Remote Support/Management of Endpoints .....	13
SD-1.11. Mobile Threat Defense (MTD).....	13
SD-1.11.1. Workspace ONE Mobile Threat Defense (MTD) .....	13
SD-1.13. Important Information.....	15
SD-1.14. Terms of Service (TOS).....	16
SD-1.15. Data Privacy .....	16
SD-2. Offer Elements (Service Components) .....	17
SD-2.1. Software .....	17
SD-2.2. Hosting.....	17
SD-2.3. Professional Services .....	17
SD-2.3.1. Mobile and Desktop Essentials Configuration and Training.....	17
SD-2.3.1.1. Deliverables .....	18
SD-2.3.1.2. Service Assumptions .....	19

SD-2.3.2. Standard Configuration and Training .....	20
SD-2.3.2.1. Deliverables .....	20
SD-2.3.2.2. Service Assumptions .....	23
SD-2.3.3. Advanced Configuration and Training .....	23
SD-2.3.3.1. Deliverables .....	24
SD-2.3.3.2. Service Assumptions .....	27
SD-2.3.4. Standard Installation and Training for Use of MDM Software (Required for the Installation of Omnissa Enterprise Mobility Software).....	29
SD-2.3.5. Advanced Installation and Training for Use of MDM Software (Required for the Installation of Omnissa Enterprise Mobility Software and a Secure Email Gateway and a Unified Access Gateway) .....	29
SD-2.3.6. Omnissa Secure Email Gateway (SEG) Implementation and Configuration .....	29
SD-2.3.6.1. Omnissa Unified Access Gateway (UAG) Implementation and Configuration (Optional) .....	29
SD-2.3.6.2. Omnissa Cloud Connector Implementation and Configuration.....	30
SD-2.3.7. Omnissa WS1 Mobile Threat Defense (MTD) Installation and Training (Add-On Service).....	30
SD-2.3.7.1. Hours of Operation .....	30
SD-2.3.7.2. Prerequisites .....	31
SD-2.3.7.3. Engagement Activities .....	31
SD-2.3.7.4. Discovery Conference .....	32
SD-2.3.7.5. Project Readiness Call.....	32
SD-2.3.7.6. Project Activity and Scope .....	32
SD-2.3.7.7. Out of Scope Items.....	32
SD-2.3.8. Omnissa WS1 Content – Advanced Installation and Training (Add-On Service to Advanced).....	33
SD-2.3.9. Customer Responsibilities Relating to Unified Endpoint Management (UEM) .....	33
SD-2.3.10. Telecom Professional Services (Optional).....	33
SD-2.3.11. Operations Training (Optional).....	34
SD-2.3.12. Managed Service Health Check (Optional) .....	34
SD-2.3.13. Certificate Integration (Optional) .....	34
SD-2.3.14. Policy Reviews for Customization (Optional).....	34
SD-2.3.15. Advanced Authentication using Certificates and Kerberos Delegation (Optional) .	35
SD-2.3.15.1. Service Scope.....	35
SD-2.3.16. Customer Service Desk (CSD) Support Plan .....	35
SD-2.3.17. Remote Administration Service Plan.....	36
SD-2.3.18. Customer On-boarding and Set Up.....	37

SD-2.4. Connection of Solution to Customer's Environment .....	37
SD-2.5. Post-Contract Support Requirements .....	37
SD-2.6. Responsibilities of the Parties.....	39
SD-2.7. Change Control .....	39
SD-2.8. Severity Levels and Initial Response Acknowledgement.....	40
SD-3. LEVELBLUE Unified Endpoint Management (UEM) Remote Administration Support (Optional) .....	40
SD-3.1. UEM Environment Discovery .....	40
SD-3.2. Consulting and Advisory Services for Remote Administration Support.....	41
SD-4. Glossary.....	42
Country Specific Provisions (CSP).....	44
CSP-2. Prohibited Countries.....	44
CSP-2.1. Device and Software Selection.....	44
CSP-2.2. Data Protection .....	44
CSP-2.3. Encryption Technology.....	45
CSP-2.4. Filters, Interception and Monitoring .....	45
CSP-2.5. Compliance with Laws.....	45
CSP-2.6. Discontinuance.....	45
CSP-2.7. Taxes.....	46
CSP-2.8. Additional Indemnification.....	46



## Omnissa Workspace ONE – CLOUD

*Section Effective Date: 21-Nov-2022*

Omnissa Workspace ONE® - CLOUD ("Workspace ONE" or "Solution") is an enterprise platform that enables Customers to manage apps on smartphones, tablets, and laptops. By integrating app access management, unified endpoint management, and near real-time application delivery, Workspace ONE is readily engaged by users, helps reduce the threat of data loss, and modernizes traditional IT operations.

The Workspace ONE editions allow organizations to use the technology based on user and endpoint requirements.

This Service Guide consists of the following parts:

- Service Description (SD)
- Pricing (P)
- Country Specific Provisions (CSP)

### Service Description (SD)

#### SD-1. General

*Section Effective Date: 21-Nov-2022*

The Solution is offered via editions that provide progressive layers to meet a customer's specific needs for features and functionality. Recurring charge subscriptions to all cloud editions include a subscription plus the Customer Service Desk (CSD) Support Plan described below. For perpetual licenses for Cloud editions, a Customer Service Desk Support Plan is required and must be purchased separately.

#### SD-1.1. Editions

##### SD-1.1.1. Essentials

##### SD-1.1.1.1. Omnissa Workspace ONE Employee Essentials Edition

*Section Effective Date: 21-Nov-2022*

Workspace ONE Employee Essentials provides Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, App Wrapping, Secure Email Gateway, Reports, Report Customization of Snapshot Data, Configurable Dashboards, Automation Engine, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, and Workspace ONE PIV-D Manager.

**SD-1.1.1.2. Omnissa Workspace ONE Mobile Essentials Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Mobile Essentials provides for mobile devices: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Mobile SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, Mobile Device Management, Basic Shared Device Management, Android OEM Extensions, Mobile App Management, App Wrapping, Mobile Email Management, Secure Email Gateway, Telecom Management Tools, Modern Desktop Management for Kiosk use cases only, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Configurable Dashboards, Automation Engine, Device Health and Lifecycle, Device Health and Security, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, Device Health and Lifecycle, Device Health and Security.

Mobile Device Management

Hub Services for UEM Notifications

Professional Services

**SD-1.1.1.3. Omnissa Workspace ONE Desktop Essentials Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Desktop Essentials provides for desktops and laptops: Workspace ONE Desktop Essentials provides for desktop/laptops: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, Secure Email Gateway, Modern Desktop Management for Kiosk use cases only, Advanced Desktop Management, Enterprise Desktop Management, Workspace ONE AirLift™ for Windows Devices, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Configurable Dashboards, Automation Engine, Device Health and Lifecycle, Device Health and Security, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, Device Health and Lifecycle, Device Health and Security.

**SD-1.1.1.4. Omnissa Workspace ONE UEM Essentials Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Unified Endpoint Management Essentials provides for all qualified endpoints: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Mobile SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, Mobile Device Management, Basic Shared Device Management, Android OEM Extensions, Mobile App Management, App Wrapping, Mobile Email Management, Secure Email Gateway, Telecom Management Tools, Modern Desktop Management for Kiosk use cases only, Advanced Desktop Management, Enterprise Desktop Management, Workspace ONE AirLift™ for Windows Devices, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Configurable Dashboards, Automation Engine,

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

---

Device Health and Lifecycle, Device Health and Security, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, Device Health and Lifecycle, and Device Health and Security.

---

**SD-1.1.2. Workspace ONE Standard Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Standard Edition provides for all qualifying endpoints: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Mobile SSO, Multifactor Authentication, Conditional Access Control, Mobile Device Management, Basic Shared Device Management, Android OEM Extensions, Mobile App Management, Mobile Email Management, Secure Email Gateway, Modern Desktop Management for Kiosk use cases only, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, and Advanced Mission Critical Device Management (Frontline Worker Add-On).

**SD-1.1.3. Workspace ONE Advanced Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Advanced Edition provides for all qualifying endpoints: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Mobile SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, Mobile Device Management, Basic Shared Device Management, Android OEM Extensions, Mobile App Management, App Wrapping, Mobile Email Management, Secure Email Gateway, Telecom Management Tools, Modern Desktop Management for Kiosk use cases only, Advanced Desktop Management, Workspace ONE AirLift™ for Windows Devices, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, and Advanced Mission Critical Device Management (Frontline Worker Add-On).

**SD-1.1.4. Workspace ONE Enterprise Edition***Section Effective Date: 21-Nov-2022*

Workspace ONE Enterprise Edition provides for all qualifying endpoints: Workspace ONE Intelligent Hub, Catalog, People, Notifications, Support, Branding, Custom Tab, Onboarding, Identity Broker, Identity Provider, Federated SSO, Mobile SSO, Multifactor Authentication, Conditional Access Control, Workspace ONE Tunnel, Mobile Device Management, Basic Shared Device Management, Android OEM Extensions, Mobile App Management, App Wrapping, Mobile Email Management, Secure Email Gateway, Telecom Management Tools, Modern Desktop Management for Kiosk use cases only, Advanced Desktop Management, Enterprise Desktop Management, Workspace ONE AirLift™ for Windows Devices, Freestyle Orchestrator, IT Compliance Automation Engine, Reports, Report Customization of Snapshot Data, Configurable Dashboards, Automation Engine, Device Health and Lifecycle, Device Health and Security, Workspace ONE SDK with DLP Protection, Workspace ONE Boxer, Workspace ONE Notebook, Workspace ONE Web, Workspace ONE Content, Workspace ONE Send, Workspace ONE PIV-D Manager, and Advanced Mission Critical Device Management (Frontline Worker Add-On),

Report Customization and scheduling (historical data), Device Health and Lifecycle, Digital Employee Experience Management, Device Health and Security, Risk Based Conditional Access with Workspace ONE Intelligence Integration, Risk Analytics, Workspace ONE Trust Network, and Virtual Apps (Horizon Universal License).

## **SD-1.2. Features Included in Editions**

### **SD-1.2.1. Workspace ONE Hub Services**

*Section Effective Date: 21-Nov-2022*

Hub Services is a set of services provided by Workspace ONE Access that adds functionality to Workspace ONE. Hub Services provides a customer's users with a single destination to access the customer's corporate resources. Hub Services includes the Workspace ONE applications catalog, notifications, and people search features. Any customer that has purchased an entitlement to Workspace ONE, either as an on-premises software offering or as a cloud service offering, can use Hub Services. Customers that have purchased an entitlement to the Workspace ONE cloud service offering can utilize Hub Services. through their existing Workspace ONE Access tenant. Hub Services is included in all editions of the Workspace ONE cloud service offering.

### **SD-1.2.2. Catalog**

*Section Effective Date: 21-Nov-2022*

Allows employees to view, install, and access configured native, mobile, SaaS and virtual applications with single sign-on (SSO) with the catalog Hub service. Curate the catalog by recommending and categorizing applications.

### **SD-1.2.3. People**

*Section Effective Date: 21-Nov-2022*

Allow employees to look up colleagues, view organization charts, view contact card, initiate calls and emails, and view your team at a glance with the people Hub service.

### **SD-1.2.4. Notifications**

*Section Effective Date: 21-Nov-2022*

Engage and communicate with all your employees with the notifications Hub service. Use the notifications builder to create and preview informational and actionable notifications that are delivered to the Workspace ONE Intelligent Hub application. Customers with Experience Workflows™ for Omnissa Workspace ONE powered by Boomi can integrate notifications with third party business systems.

### **SD-1.2.5. Support**

*Section Effective Date: 21-Nov-2022*

Give employees the ability to self-serve with on-demand access to frequently asked questions, knowledge-based articles and more as part of the brandable support section in Workspace ONE Intelligent Hub.

---

**SD-1.2.6. Branding***Section Effective Date: 21-Nov-2022*

Customize the digital workspace experience to reflect your organization's brand. Custom tab Pin a website to the navigation bar in Workspace ONE Intelligent Hub, such as a company web portal or intranet site.

**SD-1.2.7. Onboarding***Section Effective Date: 21-Nov-2022*

Provide a pre-hire onboarding experience through Workspace ONE Intelligent Hub on a web browser to give users who are recently hired access to resources before or on their start date.

**SD-1.3. Access Services****SD-1.3.1. Identity Broker***Section Effective Date: 21-Nov-2022*

Integrate with third-party identity stores and providers, including Active Directory, Azure Active Directory, LDAP, Okta and Ping.

**SD-1.3.2. Identity Provided (IdP)***Section Effective Date: 21-Nov-2022*

Serve as the identity database for user accounts.      Functionality limitations for per-device licensing mode.

**SD-1.3.3. Federated SSO***Section Effective Date: 21-Nov-2022*

Federate Active Directory to third-party or internally developed apps using one of the federation standards. Includes a password form-fill feature for SSO.

**SD-1.3.4. Mobile SSO***Section Effective Date: 21-Nov-2022*

Use certificate-based SSO for seamless launching and authentication to iOS and Android apps. On Android, SSO requires Workspace ONE Tunnel. Functionality limitations for per-device licensing mode and on-premises.

**SD-1.3.5. Multifactor Authentication (MFA)***Section Effective Date: 01-Jun-2023*

More securely access apps using Verify with Intelligent Hub, FIDO2, TOTP Authenticator Apps, or integrate third-party solutions such as RSA and Duo.

**SD-1.3.6. Conditional Access Control***Section Effective Date: 21-Nov-2022*

Utilize app access control policy to restrict access to apps based on network ranges, user groups, device platforms, applications, and authorization methods.

### **SD-1.3.7. Workspace ONE Tunnel™**

*Section Effective Date: 21-Nov-2022*

Connect apps (Omnissa or third party) to corporate intranet services with this per-app VPN client app. Requires server-side per-app VPN infrastructure, such as Omnissa Unified Access Gateway™.

### **SD-1.3.8. Workspace ONE UEM**

*Section Effective Date: 21-Nov-2022*

Workspace ONE UEM is a single solution for modern, over-the-air management of desktops, mobile, rugged, wearables, and IoT. Reduce costs, boost productivity, and deliver a great employee experience with an intelligence driven, cloud native UEM. Deliver high levels process automation, excellent device and application management, and enterprise level security at every level. Manage the full lifecycle of endpoints - mobile (Android, iOS), desktop (Windows 10 & 11, macOS), rugged and even IoT - in ONE management console to support all your end-user endpoint use cases.

### **SD-1.3.9. Workspace ONE Access**

*Section Effective Date: 21-Nov-2022*

Workspace One Access provides a number of key capabilities for Omnissa Workspace ONE® implementations, including:

- A user portal which provides browser-based access to different types of applications, including SaaS-based web applications (such as Salesforce, Dropbox, and Concur), Omnissa Horizon®-based applications and desktops, Remote Desktop Server Host (RDSH)- based applications and desktops, Omnissa Thina® -packaged apps, and Citrix based applications and desktops. The portal simplifies application access for end users with the following:
  - Enterprise identity management to sync and extend on-premises directory credentials (such as Active Directory) to SaaS and native mobile applications.
  - Enterprise Single Sign-on (SSO) to ensure that users have a single identity to log in with for internal, external, and virtual-based applications.
  - A self-service app store to allow end users to identify and be entitled to applications easily while providing enterprise security and compliance controls to ensure that the right users have access to the right applications. Workspace One Access complements the functionality of Omnissa Workspace One® UEM to deliver:
    - Device-specific authentication workflows
    - Certificate-based authentication
    - Adds additional conditional access policies including managed or unmanaged device restrictions.
    - PIN code strength and timeout enforcement, and
    - Selective Remote Wipe of installed enterprise applications.

---

## **SD-1.4. Mobile Management**

### **SD-1.4.1. Mobile Device Management**

*Section Effective Date: 21-Nov-2022*

Configure mobile device management (MDM) policies, settings and device configurations across phones, tablets and laptop devices that run iOS, Android, macOS, and Windows 10 and 11.

### **SD-1.4.2. Basic Shared Device Management**

*Section Effective Date: 21-Nov-2022*

Manage shared and kiosk configurations for mobile devices leveraging native MDM APIs, such as Android single/multi-app kiosk mode and iOS/iPadOS multiuser mode.

### **SD-1.4.4. Mobile App Management**

*Section Effective Date: 21-Nov-2022*

Install, track inventory, configure and assign apps such as internal, public, web and native apps to users and devices.

### **SD-1.4.6. Mobile Email Management**

*Section Effective Date: 21-Nov-2022*

Integrate with email infrastructure to provide access control for ActiveSync clients. Includes support for Office 365, Google Workspace, and Exchange.

### **SD-1.4.7. Secure Email Gateway (SEG)**

*Section Effective Date: 21-Nov-2022*

Provide access control to the work email server to encrypt data and attachments.

### **SD-1.4.8. Telecom Management Tools**

*Section Effective Date: 21-Nov-2022*

Track data, call and message consumption, and automate actions and compliance.

---

## **SD-1.5. Desktop Management**

### **SD-1.5.1. Modern Desktop Management**

*Section Effective Date: 21-Nov-2022*

Deliver MDM API-driven modern management of desktop operating systems. Best suited for kiosk/locked-down use cases only. Includes out-of-the-box device onboarding (OOBE, DEP); MDM-based policy configuration and OS updates; custom XML attributes and profiles; app management of modern store apps; limited MDM-based antivirus, firewall, data loss prevention (DLP), and encryption enforcement policies; and asset reporting.

### **SD-1.5.2. Advanced Desktop Management**

*Section Effective Date: 21-Nov-2022*

Deliver advanced desktop management capabilities for Windows 10 and 11, and macOS., Chrome OS and Linux beyond what is available through MDM APIs. Includes features such as drop-ship provisioning offline and online; Baselines for Group Policy Object (GPO) configuration; native desktop app lifecycle management; enterprise app repository; native peer-to-peer (P2P) app delivery; full encryption (BitLocker/FileVault) lifecycle management; Advanced Scripting Engine (supports PowerShell, Python, Bash, Zsh, etc.); Sensors for compliance reporting; granular OS patch lifecycle; Managed Admin account password escrow/auto-rotation and Filevault key escrow/auto-rotation for macOS; and more.

### **SD-1.5.3. Enterprise Desktop Management**

*Section Effective Date: 21-Nov-2022*

Deliver enterprise-level desktop management capabilities powered by Workspace ONE Intelligence™. Includes features such as OS updates automation, CVE- and Sensors-based vulnerability remediation, and others.

## **SD-1.6. IT Orchestration Framework**

### **SD-1.6.1. Freestyle Orchestrator**

*Section Effective Date: 21-Nov-2022*

Design and orchestrate complex IT workflows that consist of sequential steps with conditions based on granular criteria using a modern, low-code, canvas-based UI.

---

**SD-1.6.2. IT Compliance Automation Engine***Section Effective Date: 21-Nov-2022*

Build compliance policies with automated remediation workflows, such as app allowlist/denylist, GPS and geofencing, OS version control, and compliance escalation.

**SD-1.7. Reporting and Automation****SD-1.7.1. Reports***Section Effective Date: 21-Nov-2022*

Utilize reports in the Workspace ONE UEM console.

**SD-1.7.2. Report Customization and Scheduling (snapshot data)***Section Effective Date: 21-Nov-2022*

Design custom reports with device, application, and user data in Workspace ONE Intelligence.

**SD-1.7.3. Configurable Dashboards***Section Effective Date: 21-Nov-2022*

Get complete visibility into your digital workspace with rich visualizations at speed and scale.

**SD-1.7.5. Device Health and Lifecycle***Section Effective Date: 21-Nov-2022*

Report and automate based on device health data for mobile and desktop operating systems, including device information, Sensors, and OS updates information from Workspace ONE

**SD-1.7.6. Device Health and Security***Section Effective Date: 21-Nov-2022*

Report on threat and compliance data from sources, including Workspace ONE UEM and Workspace ONE Access™.

**SD-1.8. Mobile Productivity Apps**

---

**SD-1.8.2. Workspace ONE Boxer***Section Effective Date: 21-Nov-2022*

Give employees an all-in-one email, calendar, contacts and files experience via this highly secure, containerized mobile application, with enhanced security and productivity features built in.

**SD-1.8.4. Workspace ONE Web***Section Effective Date: 21-Nov-2022*

Give employees fast access to intranet sites and web apps via this highly secure, containerized mobile application. Includes the ability to lock devices into kiosk (single-app) mode.

**SD-1.8.5. Workspace ONE Content***Section Effective Date: 21-Nov-2022*

Enable employees to aggregate, view, and mark up files across on-premises and cloud-based file repositories via this highly secure, containerized mobile application. Includes mobile content management, file editing and annotation while protecting from data loss with cut/copy/paste/open-in restrictions.

**SD-1.8.7. Workspace ONE PIV-D Manager***Section Effective Date: 21-Nov-2022*

Enable two-factor authentication through a derived credential client certificate via this highly secure, containerized mobile application that integrates with major derived credential solution providers.

**SD-1.10. Remote Support for Endpoints****SD-1.10.1. Workspace ONE Assist for Remote Support/Management of Endpoints***Section Effective Date: 21-Nov-2022*

Enable IT and help desk staff to quickly assist employees with mobile device and laptop tasks and issues with remote view and control capabilities; advanced privacy settings; and file, task, and application management tools. Supports Android, iOS, Windows 10 and 11, and macOS.

**SD-1.11. Mobile Threat Defense (MTD)****SD-1.11.1. Workspace ONE Mobile Threat Defense (MTD)***Section Effective Date: 01-Jun-2023*

Omnissa Workspace ONE Mobile Threat Defense enables proactive mobile security by actively predicting, detecting, and helping to prevent cyber-attacks, without disturbing user privacy or disrupting users' mobile productivity.

Mobile Threat Defense helps to protect against network-based threats, malware, vulnerability exploits and other targeted attacks originating from both internal and external sources. The solution's predictive technologies leverage mobile threat intelligence gathered via massive crowd intelligence and sophisticated machine learning.

Mobile Threat Defense uses a multi-layer approach to detect malware based on parameters such

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

---

as signatures, user behavior, static/dynamic analysis, source origin, structure, permissions, and known malicious application blacklists. It also utilizes a patented proactive approach to help secure mobile devices against network-based attacks. Mobile Threat Defense uses crowd intelligence and research to help identify attacks and notify OS vendors and users of required OS upgrades or patches.

---

**SD-1.13. Important Information***Section Effective Date: 21-Nov-2022*

- A minimum of 20 Solution subscriptions is required for initial order.
- The Solution's functionality is limited to certain mobile devices and operating systems. A list of compatible devices and operating systems is available by contacting an LEVELBLUE Account Executive. Not all features are available on all devices.
- Billing begins as of Effective Date of the applicable order.
- All monies paid for the Solution are non-refundable.
- The Solution is available only to Customers with a qualified LEVELBLUE business or government agreement (Enterprise Agreement) and a Foundation Account Number (FAN).
- Availability, security/privacy, delivery, and timeliness of information are not guaranteed by LEVELBLUE.
- User based subscriptions may be applied to up to 5 devices.
- The Solution's administrative interface is accessed via a Web portal and requires a PC with Internet connection.
- The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. LEVELBLUE does not guarantee compliance with such customized settings and/or updates.
- LEVELBLUE reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without notice and without cause.
- Additional hardware, software, service, and/or network connection may be required to access the Solution. Customer's responsibilities relating to deployment of the Solution are set forth in the Customer's Responsibilities Relating to UEM Deployment section of this Service Guide.
- LEVELBLUE reserves the right to perform work remotely and use, in LEVELBLUE's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution.

- Use of the Solution requires download of application software to user devices from an app store or from a third-party site. LEVELBLUE is not licensing or furnishing the software.
- The Solution is subject to the terms and conditions of the applicable Enterprise Agreement between LEVELBLUE and Customer, the Omnissa Terms of Service (TOS) and the additional Omnissa agreements described in the "Terms of Service" section below.
- Exclusive Remedy - Customer's sole and exclusive remedy for any damages, losses, claims, costs, and expenses arising out of or relating to use of the Solution will be termination of service.

#### **SD-1.14. Terms of Service (TOS)**

*Section Effective Date: 21-Nov-2022*

Customer and its end users must enter into a separate TOS agreement with Omnissa in order to access and use the Solution. LEVELBLUE is not a party to the TOS. Omnissa is solely responsible for all items provided pursuant to that agreement. This agreement must be accepted before Customer's first use of the Solution.

If Customer does not accept the terms of the TOS, Customer must not use the Solution. Customer is responsible for all end users' performance under the TOS and agrees its end users will comply with the obligations thereunder, including but not limited to the limitations of use in certain countries. Customer is responsible for providing each end user of an enabled mobile device with a copy of the TOS.

#### **SD-1.15. Data Privacy**

*Section Effective Date: 21-Nov-2022*

Customer Personal Data may be transferred to or accessible by (i) LEVELBLUE personnel around the world; (ii) third-parties who act on LEVELBLUE's or LEVELBLUE's supplier's behalf as subcontractors; and (iii) third-parties (such as courts, law enforcement, or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users and will camouflage or securely encrypt Customer Personal Data in a manner compatible with the Solution. As used in this Service Guide, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information, or any other information that identifies or could reasonably be used to identify Customer or its end users. Customer is responsible for providing end users with clear notice of LEVELBLUE's and Customer's collection and use of Customer Personal Data obtained via the Solution and for obtaining end user consent to that collection and use.

---

**SD-2. Offer Elements (Service Components)***Section Effective Date: 16-Nov-2017*

The Solution includes rights to use Omnissa software, hosting, optional features, and Professional Services.

**SD-2.1. Software***Section Effective Date: 06-Jan-2021*

Customer and its end users' rights to use the Solution will be defined in the applicable Pricing Schedule or other ordering documents.

**SD-2.2. Hosting***Section Effective Date: 16-Nov-2017*

Hosting of the Omnissa software is provided by Omnissa on servers provided by Omnissa or its hosting suppliers ("Hosting Services"). A description of Omnissa Hosting Services and responsibilities and liabilities for those services is set forth in the TOS.

**SD-2.3. Professional Services***Section Effective Date: 01-Jun-2023*

Professional Services are performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time, excluding U.S. holidays. LEVELBLUE will attempt to accurately estimate the time required to successfully complete any projects. Customer acknowledges and agrees that if external impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of LEVELBLUE, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order form.

All Professional Service meetings are conducted remotely, unless otherwise agreed by the parties. Details regarding each Professional Services meeting can be obtained from an LEVELBLUE representative. Each such meeting may be subject to a cancellation fee of up to \$500.00 if Customer cancels less than 24 hours before the scheduled meeting.

**SD-2.3.1. Mobile and Desktop Essentials Configuration and Training***Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide implementation services connected with the purchase of the associated Omnissa software subscriptions and hosting fees. The deployment will be conducted in a Omnissa hosted environment with optional integration supported by a Omnissa Cloud Connector™ in the Customer's data centers. This project includes two meetings.

The first meeting is approximately 30 - 60 minutes and includes the LevelBlue consulting resource. The meeting is designed to provide an overview of the implementation activities for both the technical setup and functional configuration for the Customer's deployment..

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

The second meeting is up to 4 hours and is designed to install the necessary technical components to connect a customer's infrastructure to the Workspace ONE Cloud hosted environment. The meeting is also used for the installation and configuration of one Workspace ONE Cloud Connector if applicable.

**SD-2.3.1.1. Deliverables**

*Section Effective Date: 21-Nov-2022*

<b>Meeting 1: Kick-Off</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Review Customer's subscriptions and device types to be enrolled (iOS, Android, MacOS and Windows 10)		LEVELBLUE
Review Apple ID requirements for APNS certificate, Apple Business Manager (DEP and VPP)		LEVELBLUE
Review Google account requirements for Android Enterprise		LEVELBLUE
Provide available dates/times for configuration and training call	Established at the end of the kick-off call	Customer

<b>Meeting 2: Configuration and Training Deliverables Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Assistance uploading APNs certificate for iOS device management	Required only for iOS devices	LEVELBLUE with Customer
Assistance integrating Apple Business Manager with Workspace ONE (DEP and VPP)	As applicable	LEVELBLUE with Customer
Assistance integrating Google account with Workspace ONE for Android Enterprise	As applicable	LEVELBLUE with Customer
Assistance integrating Samsung KME with Workspace ONE	As applicable	LEVELBLUE with Customer
Assistance integrating Google Zero-touch with Workspace ONE	As applicable	LEVELBLUE with Customer
User Management: Review creation of admin accounts and user accounts (up to 5 accounts)		LEVELBLUE with Customer
Assist creating up to 2 child organization groups	If applicable	LEVELBLUE with Customer

<b>Meeting 2: Configuration and Training Deliverables Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

Assist creating up to 2 smart groups	If applicable	LEVELBLUE with Customer
Enroll up to 3 devices (iOS, Android, MacOS, Windows 10) Review device dashboard actions and review device commands and use cases	Customer must bring devices to this meeting	LEVELBLUE with Customer
Applications: Configure App Catalog Add 3 iOS, Android, MacOS, Windows 10 recommended/purchased apps PS team will show the SDK access in the portal and show customer the links where additional info is available		LEVELBLUE with Customer
Profiles: Create up to 3 profiles and assign to devices (includes email profile)		LEVELBLUE with Customer
Assist creating up to 1 compliance policies including email compliance policies if applicable	If applicable	LEVELBLUE with Customer
Review reporting capabilities		LEVELBLUE with Customer
Assist in configuring Intelligent Hub Services: Notifications Support/Self-Service Branding Custom Tab		LEVELBLUE with Customer
Administration: Review overall portal navigation Explain help links and online resources		LEVELBLUE with Customer
Onboard customer to LEVELBLUE support desk		LEVELBLUE
Send post implementation customer survey		LEVELBLUE

**SD-2.3.1.2. Service Assumptions**

*Section Effective Date: 21-Nov-2022*

Alignment of all UEM configurations and policy design with Customer's requirements is the responsibility of Customer. Procurement, configuration, and installation of hardware is the responsibility of Customer. LEVELBLUE will provide configuration recommendations or suggest best practices.

All work, documentation and work product(s) will be conducted during normal business hours and will be provided in English.

**SD-2.3.2. Standard Configuration and Training***Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide implementation services connected with the purchase of the associated Omnissa software subscriptions and hosting fees. The deployment will be conducted in a Omnissa hosted environment with optional integration supported by a Omnissa Cloud Connector™ in the Customer's data centers. This project includes two meetings.

- The first meeting is approximately 30 - 60 minutes and includes the Managed Services professional consulting resource. The meeting is designed to provide an overview of the implementation activities for both the technical setup and functional configuration for the Customer's deployment. The topics covered are focused on the preparation for technical installation of system components, on the scope of the features available/recommended, and the pre-installation expectations of the Customer's infrastructure/environment.
- The second meeting is up to 4 hours and is designed to install the necessary technical components to connect a customer's infrastructure to the Workspace ONE Cloud hosted environment, to configure the recommended features for Customer's project, and to deploy an initial pilot set of devices. The meeting is also used for the installation and configuration of one Workspace ONE Cloud Connector.

**SD-2.3.2.1. Deliverables***Section Effective Date: 21-Nov-2022*

<b>Meeting 1: Kick-Off</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Review Customer's subscriptions and device types to be enrolled (iOS, Android, and Windows)		LEVELBLUE
Review Cloud Connector server virtualization requirements, networking/firewall		LEVELBLUE
Review Apple ID requirements for APNS certificate, Apple Business Manager (DEP and VPP)		LEVELBLUE
Review Google account requirements for Android Enterprise		LEVELBLUE
Review Active Directory service account needed for directory lookups		LEVELBLUE
Provide available dates/times for configuration and training call	Established at the end of the kick-off call	Customer

<b>Meeting 2: Standard Configuration and Training Deliverables Customer-provided Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Installation of Workspace ONE Cloud Connector software		LEVELBLUE with Customer

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

Assist Active Directory configuration (Service Account)		Customer
---	--	----------

<b>Meeting 2: Standard Configuration and Training Deliverables Customer-provided Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Assistance uploading APNs certificate for iOS device management	Required only for iOS devices	LEVELBLUE with Customer
Assistance integrating Apple Business Manager with Workspace ONE (DEP and VPP)	As applicable	LEVELBLUE with Customer
Assistance integrating Google account with Workspace ONE for Android Enterprise	As applicable	LEVELBLUE with Customer
Assistance integrating Samsung KME with Workspace ONE	As applicable	LEVELBLUE with Customer
Assistance integrating Google Zero-touch with Workspace ONE	As applicable	LEVELBLUE with Customer
User Management: Review creation of admin accounts and user accounts (up to 5 accounts)		LEVELBLUE with Customer
Assist creating up to 2 child organization groups	If applicable	LEVELBLUE with Customer
Assist creating up to 2 smart groups	If applicable	LEVELBLUE with Customer
Assist with enrolling up to 5 devices total (iOS, Android, Windows 10, or Macintosh) Enroll up to 5 devices (iOS, Android, or Windows 10, or Macintosh) Review device dashboard actions and review device commands and use cases	Customer must bring devices to this meeting	LEVELBLUE with Customer
Applications: Configure App Catalog Add up to 2 iOS and/or Android recommended/purchased apps Add up to 1 in-house app		LEVELBLUE with Customer
Profiles: Create up to 3 profiles and assign to devices		LEVELBLUE with Customer
Assist integrating PowerShell Email Management	If applicable	LEVELBLUE with Customer

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

Assist creating up to 2 compliance policies including email compliance policies if applicable	If applicable	LEVELBLUE with Customer
Configure Boxer email client	If applicable	LEVELBLUE with Customer
Review reporting capabilities		LEVELBLUE with Customer

Meeting 2: Standard Configuration and Training Deliverables Customer-provided Devices ARE Required for this Meeting		
Deliverables	Notes	Owner
Administration: Review overall portal navigation Explain help links and online resources		LEVELBLUE with Customer
Onboard customer to LEVELBLUE support desk		LEVELBLUE
Send post implementation customer survey		LEVELBLUE

### SD-2.3.2.2. Service Assumptions

*Section Effective Date: 21-Nov-2022*

- Alignment of all UEM configurations and policy design with Customer's requirements is the responsibility of Customer. Procurement, configuration, and installation of hardware is the responsibility of Customer. LEVELBLUE will provide configuration recommendations via a checklist.
- All work, documentation and work product(s) will be conducted during normal business hours and will be provided in English.
- LEVELBLUE will only configure the Workspace ONE Cloud Connector to integrate with Microsoft Active Directory Configuration.
- The following Workspace ONE Cloud special feature configuration activities are excluded and out of scope:
  - SCEP and certificate usage
  - PKI integration/Kerberos
  - Azure AD integration for authentication
  - SAML

### SD-2.3.3. Advanced Configuration and Training

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide installation and training services connected with the purchase of the associated Omnissa software subscriptions. The installation and training services will include an Omnissa Cloud Connector, a Secure Email Gateway integration for email management, a Unified Access Gateway (UAG) for Content Management or Secure Browsing, as well as installation, configuration, and training services for Omnissa Access. These services consist of a total of four meetings.

- The first meeting is approximately 30 - 60 minutes and includes the Managed Services professional consulting resource. The meeting is designed to provide an overview of the implementation activities for both the technical setup and functional configuration for the Customer's deployment. The topics covered are focused on the preparation for technical

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

installation of system components, on the scope of the features available/recommended, and the pre-installation expectations of the Customer's infrastructure/environment.

- The second meeting is approximately 30 minutes and is designed to ensure the Customer has completed the pre-installation requirements for the system components (servers, firewall rules, service accounts, TLS certificates, etc.).
- The third meeting is approximately 120 minutes and is designed to install the technical components necessary to deploy the Workspace ONE Solution in the Customer's infrastructure.
- The fourth meeting is approximately 5-6 hours and is designed, to configure the recommended features for the Customer's project, and to deploy an initial pilot set of devices.

**SD-2.3.3.1. Deliverables**

*Section Effective Date: 21-Nov-2022*

<b>Meeting 1: Kick-Off</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Review Customer's subscriptions and device types to be enrolled (iOS, Android, and Windows)		LEVELBLUE
Review server virtualization requirements, networking/firewall for all components		LEVELBLUE
Review Apple ID requirements for APNS certificate, Apple Business Manager (DEP and VPP)		LEVELBLUE
Review Google account requirements for Android Enterprise		LEVELBLUE
Review Active Directory service account needed for directory lookups		LEVELBLUE
Provide available dates/times for configuration and training call	Established at the end of the kick-off call	Customer
Provide available dates/times for readiness call	Established at the end of the kick-off call	Customer

<b>Meeting 2: Readiness</b>		
<b>Responsibilities</b>	<b>Notes</b>	<b>Owner</b>
Review Customer Pre-Deployment Checklist	Workbook delivered in e-mail to Customer	Customer
Provide available dates/times for configuration and training call	Established at the end of the readiness call	Customer

<b>Meeting 3: Advanced Configuration and Training Deliverables Customer-provided Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Installation of Workspace ONE Cloud Connector software		LEVELBLUE with Customer
Assist Active Directory configuration (Service Account)		Customer
Installation of UAG (content gateway/tunnel)	If applicable	LEVELBLUE with Customer
Installation of SEG (secure email gateway)	If applicable	LEVELBLUE with Customer
Configure Workspace ONE Access for identity management	If applicable	LEVELBLUE with Customer
Assist client with deploying up to 2 SAML applications via Access	If applicable	LEVELBLUE with Customer
Enroll up to 3 devices within Workspace ONE, deploy Workspace ONE app, verify user can login.	If applicable	LEVELBLUE with Customer
Assistance uploading APNs certificate for iOS device management	Required only for iOS devices	LEVELBLUE with Customer
Assistance integrating Apple Business Manager with Workspace ONE (DEP and VPP)	As applicable	LEVELBLUE with Customer
Assistance integrating Google account with Workspace ONE for Android Enterprise	As applicable	LEVELBLUE with Customer
Assistance integrating Samsung KME with Workspace ONE	As applicable	LEVELBLUE with Customer
Assistance integrating Google Zero-touch with Workspace ONE	As applicable	LEVELBLUE with Customer
User Management: Review creation of admin accounts and user accounts (up to 5 accounts)		LEVELBLUE with Customer
Assist creating up to 2 child organization groups	If applicable	LEVELBLUE with Customer
Assist creating up to 2 smart groups	If applicable	LEVELBLUE with Customer

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

<p>Assist with enrolling up to 5 devices total (iOS, Android, Windows 10, or Macintosh)          Enroll up to 5 devices (iOS, Android, or Windows 10, or Macintosh)          Review device dashboard actions and review device commands and use cases</p>	<p>Customer must bring devices to this meeting</p>	<p>LEVELBLUE with Customer</p>
---	--	--------------------------------

<b>Meeting 3: Advanced Configuration and Training Deliverables Customer-provided Devices ARE Required for this Meeting</b>		
<b>Deliverables</b>	<b>Notes</b>	<b>Owner</b>
Applications: Configure App Catalog Add up to 2 iOS and/or Android recommended/purchased apps Add up to 1 in-house app		LEVELBLUE with Customer
Profiles: Create up to 3 profiles and assign to devices		LEVELBLUE with Customer
Assist integrating PowerShell Email Management	If applicable	LEVELBLUE with Customer
Assist creating up to 2 compliance policies including email compliance policies if applicable	If applicable	LEVELBLUE with Customer
Configure Boxer email client, Omnissa Web, Workspace ONE Content	If applicable	LEVELBLUE with Customer
Configure Telecom	If applicable	LEVELBLUE with Customer
Review reporting capabilities		LEVELBLUE with Customer
Administration: Review overall portal navigation Explain help links and online resources		LEVELBLUE with Customer
Onboard customer to LEVELBLUE support desk		LEVELBLUE
Send post implementation customer survey		LEVELBLUE

### **SD-2.3.3.2. Service Assumptions**

*Section Effective Date: 01-Jun-2023*

- Alignment of all UEM configurations and policy design with Customer's requirements is the responsibility of Customer. Procurement, configuration, and installation of hardware is the responsibility of Customer. LEVELBLUE will provide configuration recommendations via a checklist.
- All work, documentation and work product(s) will be conducted during normal business hours and will be provided in English.
- LEVELBLUE will only configure the Workspace ONE Cloud Connector to integrate with Microsoft Active Directory Configuration. Lotus Notes is not supported.

- The following Workspace ONE Cloud special feature configuration activities are excluded and out of scope:

- SCEP and certificate usage
- PKI integration/Kerberos

#### **SD-2.3.4. Standard Installation and Training for Use of MDM Software (Required for the Installation of Omnissa Enterprise Mobility Software)**

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide installation and training services connected with the purchase of the associated Omnissa software subscriptions. The installation and training services will include installation of necessary components.

#### **SD-2.3.5. Advanced Installation and Training for Use of MDM Software (Required for the Installation of Omnissa Enterprise Mobility Software and a Secure Email Gateway and a Unified Access Gateway)**

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide installation and training services connected with the purchase of the associated Omnissa software subscriptions. The installation and training services will include installation of components located on the Customer's premises, including the Console, an optional Omnissa Cloud Connector, either a Secure Email Gateway or PowerShell integration for email management, a Unified Access Gateway for Content Management or Browser, as well as installation, configuration, and training services for Omnissa Identity Manager.

#### **SD-2.3.6. Omnissa Secure Email Gateway (SEG) Implementation and Configuration**

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will install, configure, and test the SEG. Workspace ONE supports multiple types of email management, ranging from the remote configuration of supported email clients on devices to a robust compliance infrastructure. The Secure Email Gateway (SEG) is a highly secure, on-premises email proxy that sits between the mobile devices and the email server, blocking or allowing email access according to a set of customizable rules. PowerShell integration has similar functionality, usually without an on-premises component. Remote email configuration is not contingent on either of these optional features, email integration w/exchange and Office 365 can be implemented via workspace one profiles.

##### **SD-2.3.6.1. Omnissa Unified Access Gateway (UAG) Implementation and Configuration (Optional)**

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will remotely configure and integrate one UAG into the Omnissa environment. Setup will include integration with one or all of the following: (i) internal document repositories and content using the WS1 Content; (ii) internal websites using the Workspace ONE Browser; and (iii) internal web applications with access to internal resources.

The UAG acts as a proxy host for connections inside a Customer's trusted network. This design provides an extra layer of security by shielding virtual desktops, application hosts, and servers from the public-facing Internet.

#### **SD-2.3.6.2. Omnissa Cloud Connector Implementation and Configuration**

*Section Effective Date: 06-Jan-2021*

LEVELBLUE will remotely configure and integrate one cloud connector on the Customer's premises. Setup will include integration to one Active Directory server. Customer is responsible for provisioning a server on its premises in accordance with the configuration checklist to be provided.

#### **SD-2.3.7. Omnissa WS1 Mobile Threat Defense (MTD) Installation and Training (Add-On Service)**

*Section Effective Date: 01-Jun-2023*

LEVELBLUE's professional services consultants ("Consultants") will assist customer's using support technology platforms to complete the following related platform integration to their Unified Endpoint Management (UEM) or Mobile Threat Defense (MTD) environments:

Service will include discussion, review, and demonstration of all the knowledge topics, workflows and configurations related to completing the integrations or training topics selected above.

##### **SD-2.3.7.1. Hours of Operation**

*Section Effective Date: 01-Jun-2023*

LEVELBLUE Professional Services will be performed during normal business hours in the Consultant's time zone, Monday through Friday, excluding U.S. holidays, and must be completed within a

timeframe as specified in the Rate Table below. Customer must provide LEVELBLUE access to the environment and ensure that appropriate resources with access to that environment are made available during performance of the services as needed.

### **SD-2.3.7.2. Prerequisites**

*Section Effective Date: 01-Jun-2023*

As prerequisite for this service, LEVELBLUE may remotely perform an inspection of the Customer's existing environment. The purpose of the inspection is to review the current state of the Customer's environment and the environment's configuration and settings. This discovery effort will provide a baseline for consulting. The inspection is performed remotely and there are no travel expenses required or included.

Additionally, the customer must:

- Complete the pre-implementation checklist if one is required.
- Supply up to three devices to be used to verify and demonstrate the integration.
- Complete enrollment in relevant vendor programs related to the engagement.
- Any other service-specific prerequisites related to the engagement topic not listed above. Consultant may provide Customer a task list to complete prior to the first engagement encounter.
- Access to the UEM/MTD and related tenants and portal user interfaces, under supervision by the Customer, during the engagement sessions using an agreed upon web conferencing application for screen sharing.
- Provide LEVELBLUE with two technical contacts who are authorized to work with the LEVELBLUE Professional Services Consultant during the project.

Note: LEVELBLUE may decline to support use cases where known problems have been identified, or when the vendor has historically declined to fully support the use case.

### **SD-2.3.7.3. Engagement Activities**

*Section Effective Date: 01-Jun-2023*

LEVELBLUE will provide the Customer with an assigned Consultant. The Consultant will be accessible via telephone and email. A designated backup will be assigned in appropriate situations. The Consultant will interface with up to two authorized Customer representative(s), who are typically IT or Security personnel responsible for the Customer's UEM production environment. LEVELBLUE will report hours used to provide the consulting service on monthly basis.

LEVELBLUE will conduct the following activities during the Access Implementation Service:

- Project Kick-off and Discovery Conference (approximately 30 minutes).
- Project Readiness Call (if requested, usually approximately 30 minutes).
- One or more Engagement Activity sessions as needed to exhaust the hours purchased.

---

**SD-2.3.7.4. Discovery Conference***Section Effective Date: 01-Jun-2023*

During the discovery conference LEVELBLUE will discuss project requirements, review prerequisites for the project, and provide an overview of the engagement methodology.

LEVELBLUE will confirm the current state of the customer's UEM/MTD configuration before initiating any configuration changes.

All work will be done remotely and over the web. LEVELBLUE will host a remote screen sharing session during the implementation and the customer must provide an administrative workstation with proper software and access to perform the tasks necessary to complete the implementation in the various UEM, MTD, and other tenants and portals.

If outstanding customer work items are identified, a short project readiness call will be scheduled, otherwise the implementation call will be scheduled at the end of the discovery conference.

**SD-2.3.7.5. Project Readiness Call***Section Effective Date: 01-Jun-2023*

If outstanding work items were identified during the discovery conference, they will be reviewed and confirmed complete. When confirmed complete, the engagement activity sessions will be scheduled.

**SD-2.3.7.6. Project Activity and Scope***Section Effective Date: 01-Jun-2023*

During the project, LEVELBLUE will provide consulting services related to the pre-agreed topics.

**SD-2.3.7.7. Out of Scope Items***Section Effective Date: 01-Jun-2023*

The following tasks are not in scope for these LEVELBLUE Professional Services:

- Any request that is not currently in the LEVELBLUE UEM Professional Service offer portfolio contained in this service guide.
- Any technical issues related to break/fix, troubleshooting and support topics.
- Installing UEM hardware or software.
- Consulting on new mobile operating systems or UEM features before they are made available.
- Consulting related to UEM vendors or products not supported by LEVELBLUE or not in production in the Customer's environment.
- Support or troubleshooting for third party applications.
- Documenting of Customer processes or support guides.
- Configuring or reconfiguring end user devices for deployment or redeployment.

Note: LEVELBLUE may refer a customer desiring comprehensive administration training to alternate service offerings targeting that training specifically.

### **SD-2.3.8. Omnissa WS1 Content – Advanced Installation and Training (Add-On Service to Advanced)**

*Section Effective Date: 21-Nov-2022*

LEVELBLUE will provide implementation services connected with the purchase of the associated Omnissa software subscriptions and applicable Hosting Fees. The deployment will be conducted in a Customer hosted environment with integration provided by an existing Mobile Access Gateway. This project includes two meetings.

### **SD-2.3.9. Customer Responsibilities Relating to Unified Endpoint Management (UEM)**

*Section Effective Date: 21-Nov-2022*

This section identifies the Customer actions required to prepare for UEM deployment. A meeting is strongly recommended in advance of the installation start date to review server configuration and reach agreement on which specific features should be implemented.

At a high level, these actions include:

- Allocating IP addresses and Fully Qualified Domain Names (FQDNs) for the platform. The IP addresses and FQDNs must be publicly accessible so mobile devices can access these platforms over the Internet.
- Ensuring access to Domain Name System (DNS) servers.
- If Lightweight Directory Access Protocol (LDAP) operation is desired, providing credentials for a system account allowing directory lookups.
- Opening required TCP and UDP ports on the firewall and communicating the necessary details during the pre-installation call with LEVELBLUE.
- Acquiring and/or preparing required certificates including the certificate for Apple Push Notification Service (APNS).
- If using virtual machines (VMs), configuring VMs that meet the provided specifications and uploading the Omnissa installation file(s) to the VM data store(s).
- Providing LEVELBLUE's technical consultant remote access to the installation environment.
- Access to the fee-based Apple Developer Program is required for the creation of the application signing certificate.

### **SD-2.3.10. Telecom Professional Services (Optional)**

*Section Effective Date: 25-Jun-2020*

LEVELBLUE will provide implementation services connected with the purchase of Telecom. The deployment will be conducted in an existing Omnissa hosted environment. This project consists of one meeting conducted remotely.

---

**SD-2.3.11. Operations Training (Optional)***Section Effective Date: 21-Nov-2022*

LEVELBLUE will conduct knowledge share and training for Customer's technical staff on the Solution. The engagement is up to five hours in duration. The training is delivered remotely via web conference and includes Customer hands-on configuration of these four features: (i) Boxer container setup; (ii) App Wrapping of one Customer developed application; (iii) Web; and (iv) Content on the Omnisca cloud Platform, as applicable. Presentation Topics that can be selected by the Customer include: User Management; Device Registration and Retirement: Policy Management and Security; Device Configuration Management; and Reports and Logs. LEVELBLUE will coordinate the web conference and a pre-call will be set-up with the Customer by LEVELBLUE to review the session agenda and logistics. All server software installation must have been completed prior to this training. Software upgrades are not offered with this service.

**SD-2.3.12. Managed Service Health Check (Optional)***Section Effective Date: 21-Nov-2022*

LEVELBLUE will inspect and review the current state of the Omnisca UEM platform and validate that the server, software implementation, and configuration are consistent with the managed solution platform vendor and LEVELBLUE best practices and recommendations. The Health Check is typically delivered remotely over two days by an LEVELBLUE Professional Services Consultant. No travel expenses are required. No hardware or software installation will be done on the Customer's premises. Any changes in scope that arise from discovery during the Health Check will be addressed via a separate professional service engagement. Included are the following: a methodological review of the existing Omnisca implementation; a review of platform configurations through inspection of configuration export (.XML) reports and/or the graphical configuration settings within the Console; a review of configuration policy definitions for error and completeness and a review of Device Status (pending, verified and wiped) and documentation of outstanding devices that should be under management. Policies are not reviewed for security efficacy. The following are also excluded: assessment of the state of the identity (Active Directory), collaboration (Exchange), or public key (certificates/SCEP) infrastructures, and implementation of any remediation recommended by the review.

Managed Health Check and System validation is provided remotely by one LEVELBLUE consultant. No hardware or software installation will be done on the Customer's premises.

**SD-2.3.13. Certificate Integration (Optional)***Section Effective Date: 16-Nov-2017*

LEVELBLUE will implement and configure the integration settings to enable Omnisca to issue certificates to mobile devices from the Customer's Microsoft Certificate authority.

**SD-2.3.14. Policy Reviews for Customization (Optional)***Section Effective Date: 16-Nov-2017*

Mobility Policy Reviews are available on a custom basis through LEVELBLUE Professional Services.

---

**SD-2.3.15. Advanced Authentication using Certificates and Kerberos Delegation (Optional)***Section Effective Date: 16-Nov-2017*

All Professional Service meetings are conducted remotely, unless otherwise agreed by the parties. Details regarding each Professional Services meeting can be obtained from an LEVELBLUE representative. Each such meeting is subject to a cancellation fee of up to \$500.00 if Customer cancels less than 24 hours before the scheduled meeting.

**SD-2.3.15.1. Service Scope***Section Effective Date: 28-Apr-2018*

LEVELBLUE will implement and configure the integration settings to enable the Solution to push certificates to mobile devices from a supported interface to the Customer's Certificate Authority. In completing the Certificate Authority integration LEVELBLUE will:

- Create one certificate template representing the Customer's desired type of identity certificate
- Define one device policy profile for Exchange ActiveSync auto-configuration using an MDM-pushed identity certificate
- Define one device policy profile for VPN Customer auto-configuration using an identity certificate
- Define one device policy profile for preferred Wi-Fi network auto-configuration using an identity certificate
- Configure the service accounts in Active Directory (User or Computer object) for Kerberos authentication delegation and create service principal names ("SPNs") if necessary
- Configure the email proxy service to request Kerberos delegated credentials on behalf of device users for mailbox access

LEVELBLUE will assist with the testing of each device profile on a single supported device.

Diagnosis and remediation of failed test cases to verify that a certificate of the correct type is issued by the Certificate Authority and installed within the device certificate store. The Customer is responsible for any diagnosis or remediation of authentication or authorization failures within the authentication, authorization, and accounting ("AAA") infrastructure.

**SD-2.3.16. Customer Service Desk (CSD) Support Plan***Section Effective Date: 01-Jun-2023*

LEVELBLUE's Support provides a Customer Service Desk (CSD) for help-desk to help-desk support. CSD is a single point of contact for Customers where requests are clarified, documented, and triaged with the appropriate service owner for resolution. While multiple parties may participate in the resolution of an issue, the CSD organization retains overall ownership to ensure a consistent customer experience. The following components are provided for Customer Service Desk:

- Technical Support

- MACD (moves, adds, changes, disconnects) Administration
- Service Optimization
- 24x7 Coverage (as described below)
- Annual Health Check (optional)

CSD 24x7 Support is included with all Omnissa Workspace ONE software bundle subscriptions.

The CSD 24x7 Support serves Customers that provide the day-to-day administration of their UEM platform. It includes:

- Help desk to help desk (Tier 2) technical support 24x7x365.
- Support to triage, escalate and attempt to resolve service issues and support requests.
- Single point of contact for Tier 2 and above support to address interoperability between carriers serving mobile devices, networks, UEM platform, mobile applications, and the hosted infrastructure.
- How-To (ad-hoc training) and FAQ support for UEM platform use, configuration, and best practices.

### **SD-2.3.17. Remote Administration Service Plan**

*Section Effective Date: 01-Jun-2023*

The LEVELBLUE Remote Administration Service Plan is a comprehensive program available at either a Basic or Advanced level that is designed for organizations that have limited internal support resources and mobile expertise. LEVELBLUE will hire, train, and maintain the staff needed to administer the Customer's UEM platform and provide a UEM consultant to assist the Customer.

In addition to the services included in the CSD 24x7 Support Plan, the Remote Administration Service Plan includes:

- A solution for which LEVELBLUE provides comprehensive daily, ongoing configuration and lifecycle administration of the UEM platform that includes user management, policy management, device configuration management and app and content management. In addition, Customer has access to the UEM administration interface for the following: Dashboard View, Verify Device Enrollment or Registration, Passcode Reset/Unlock, Lock Device, Locate/Find, Send Messages, Run/Create Reports, Add/Delete Users, Device Enrollment (Bulk or Individual), and Wipe.
- An assigned UEM consultant who will provide recommendations and ongoing consultation on Customer's UEM design, implementation, and administration.
- Support that enables Customer to update security policies and authorized device configurations.
- Annual performance Health Checks for Customer installations with at least 500 devices.

Customer is solely responsible for its employees', agents', and subcontractors' use of the UEM administration interface, including, without limitation, the enrollment and retirement of UEM device users.

Remote administration is available Monday through Friday 7:30 a.m. to 5:30 p.m. Eastern Time zone, excluding U.S. holidays.

### **SD-2.3.18. Customer On-boarding and Set Up**

*Section Effective Date: 16-Nov-2017*

LEVELBLUE will provide installation of the Solution, including: coordination of all Kickoff Call, Readiness Call, Help Desk On-boarding Call and weekly status calls; creation and maintenance of Project Schedule; coordination of LEVELBLUE and Customer resources through use of a Project Manager; and coordination of all required documentation, including a Redeployment Checklist; an Installation Questionnaire; a Project Timeline; Project Surveys; Project sign off; and a Help Desk on-boarding packet that contains all contact and escalation details for logging a ticket after installation, as well as Customer's outbound call details.

### **SD-2.4. Connection of Solution to Customer's Environment**

*Section Effective Date: 16-Nov-2017*

The connection between the solution and Customer's environment is via the Internet using secure sockets layer ("SSL"). No virtual private network ("VPN") infrastructure is required.

### **SD-2.5. Post-Contract Support Requirements**

*Section Effective Date: 16-Nov-2017*

- LEVELBLUE will assign a designated LEVELBLUE Project Manager to interface directly with Customer's designated Project Manager. LEVELBLUE and Customer shall cooperate to define an agreeable Project Plan. LEVELBLUE and Customer shall use commercially reasonable efforts to meet the timelines in the Project Plan. If LEVELBLUE or Customer cannot meet a date specified in the Project Plan, that party shall notify the other party, and the parties will agree upon revised dates for the Project Plan. Delays in Customer deliverables, including requirements, shall extend LEVELBLUE's due dates for LEVELBLUE deliverables on a day-for-day basis.
- The Customer Project Manager shall represent Customer regarding selected work activities. The Customer Project Manager is responsible for overall project management and must have the authority to direct Customer's personnel and Customer's vendors (collectively "Customer Project Team") to provide the information and to participate in, and perform, the activities required by LEVELBLUE in support of its performance under the Customer's Service Agreement. The LEVELBLUE Project Manager shall lead the LEVELBLUE Project Team, receive Change Requests and facilitate resolution of all inter-team issues encountered by the Customer Project Team or LEVELBLUE Project Team, whether arising from the performance of the parties under the Customer's Service Agreement or a Change Request.
- Customer shall designate, within 24 hours of the Effective Date of the applicable Pricing Schedule or other ordering document, Customer's relevant management, staff and vendors who may be called upon to provide information to LEVELBLUE regarding the: (i) operational and technical specifications of the Solution (ii) definition of operational requirements (iii)

.deployment of applications; and (iv) general business planning as applicable to the development of the project.

- Upon completion of Professional Services, Customer must either sign the acceptance document LEVELBLUE presents or provide within five business days of the service completion date written notice to LEVELBLUE identifying any non-conforming Professional Services. If Customer fails to provide such notice, Customer is deemed to have accepted the Professional Services.
- The LEVELBLUE Project Team may consist of an LEVELBLUE Technical Project Manager.
- The LEVELBLUE and Customer Project Managers shall participate in all phases of the project. They shall initiate the project, prepare reports, and manage project staffing, deployment, and overall delivery assurance. The LEVELBLUE Project Manager's responsibilities are as follows:
  - Conduct a formal project kick-off meeting ("Project Kick-off Meeting") which will include, among other things, concurrence from all as to the scope of the installation project. The LEVELBLUE Project Manager will work with the Customer Project Manager to create a communication plan that identifies both LEVELBLUE and Customer resources required for the project.
  - Serve as the primary interface to the Customer through the Customer's Project Manager.
  - Coordinate the site installation priorities and the installation schedules with the Customer Project Manager. The LEVELBLUE Project Manager will create an installation project timeline draft and submit the draft to Customer via hardcopy or electronic format. Customer and LEVELBLUE will mutually agree to the project timeline, and once that occurs, the project timeline will be considered final and subject to changes only through a Change Request.
  - Function as the escalation point for issues arising from the ordering and installation of the Solution.
  - Provide, at the Customer's request, email, or telephone status updates as to the progress of the implementation.
  - Participate in and schedule regular status and project planning meetings as required. The audience for such status meetings may include LEVELBLUE personnel, third-party vendors, or Customer-designated team members.
  - Develop, manage, and track project schedules and all change control processes.
  - Develop and maintain any contact list and communication plan and track and monitor prioritized action items and an issues list.
  - Manage the Test and Turn-up of the production environment.

**SD-2.6. Responsibilities of the Parties**

Section Effective Date: 21-Nov-2022

<b>Responsibilities of the Parties</b>		
<b>Task/Function</b>	<b>LEVEL BLUE</b>	<b>Customer (or Customer's Third Party)</b>
Conduct a formal project kick-off meeting. During the meeting LEVELBLUE and Customer will: introduce key people at Customer and LEVELBLUE; exchange contact information for regular reporting and emergencies; review scope of services; review communication, notification and issue escalation procedures; discuss other specific Customer requests and rules for engagement (e.g., period during which LEVELBLUE should not perform testing); and discuss the involvement of Customer's technical staff in the project for the purpose of knowledge transfer and security	R	A
Overall Project Plan and Milestones	R	C
Provide a project manager to serve as a single point of contact	R	R
Provide points of contact as requested including a designated decision-maker and company org chart		R
Provide a hand-off package upon Customer acceptance that includes LEVELBLUE Support information	R	
Provide completed questionnaires: SSL certificate, network, and DNS		R
Delivery of mobile application solution to end-users' devices		R
Install, configure, and maintain subscriptions or licenses that Customer has procured through LEVELBLUE as part of the Solution	R	
Provide administrator education and implement policy administration of end user groups within the Solution	R	
User acceptance testing prior to environment go-live	C	R
Notes: R = Responsible, C = Consult and A = Assist		

**SD-2.7. Change Control**

Section Effective Date: 16-Nov-2017

LEVELBLUE and Customer will manage all Changes through a written change request process ("Change Control Process"). Either Party must submit change requests in writing to the other party via LEVELBLUE's required process.

The party requesting the Change must submit a written change request to the other party and the receiving party shall issue a written response to the change request, including whether the receiving party accepts or rejects the request.

**SD-2.8. Severity Levels and Initial Response Acknowledgement***Section Effective Date: 16-Nov-2017*

<b>Severity Levels and Initial Response Acknowledgement</b>		
<b>Label</b>	<b>Definition</b>	<b>Initial Response Time Target</b>
Severity 1	System is down or completely inoperable and has more than one of the following characteristics: A complete loss of the service or unable to administer the system; No interim restoration or workaround is possible.	30 minutes
Severity 2	Product operating in reduced capacity or partially unavailable and has more than one of the following characteristics: Loss or critical functionality / service or ability to administer the system; No interim restoration or workaround is possible.	30 minutes
Severity 3	A Trouble that has a non-critical functionality loss or minor impact on service for End Users. Single end user issue. Workaround exists.	30 minutes

**SD-3. LEVELBLUE Unified Endpoint Management (UEM) Remote Administration Support (Optional)***Section Effective Date: 01-Jun-2023*

LEVELBLUE's UEM consultants (Consultants) will perform advanced security and UEM policy analysis and provide recommendations based on industry best practices for UEM design, implementation and administration based upon Customer's use of the Solution platform. Services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., Customer's local time. All services are provided in English.

**SD-3.1. UEM Environment Discovery***Section Effective Date: 06-Jan-2021*

LEVELBLUE will remotely perform an inventory of the Customer's existing UEM environment. The purpose of the inventory is to document the current state of the Customer's UEM environment and the environment's configuration and settings. This discovery effort will generate a report and provide a baseline for consulting. The inventory is performed remotely and there are no travel expenses required or included. Services will be performed Monday through Friday during mutually agreed hours and must be completed within 30 days of order placement. Customer must provide LEVELBLUE access to its UEM environment and ensure that appropriate resources with access to that environment are made available during the entire inventory process.

---

**SD-3.2. Consulting and Advisory Services for Remote Administration Support***Section Effective Date: 01-Jun-2023*

LEVELBLUE will assign a consultant familiar with the Customer's baseline report and expertise in the Customer's UEM environment. The Consulting Services will be provided for the Customer's current UEM environment and includes best practices and consulting on how to perform UEM administration or system configuration changes such as the following:

- Organizational strategies and structure of users within the UEM environment
- User management strategies
- Security policy configuration and options
- Device configuration profiles
- Connectivity configuration profiles (e.g., Wi-Fi, VPN)
- Application management and distribution
- Content management and distribution.
- Growing and scaling the UEM platform and user base
- Additional integration into the Customer's environment (LDAP, Exchange, Certificates)
- New UEM features and functionality

Access to the assigned Consultant must be scheduled in advance and is available Monday through Friday at mutually agreed upon times during Customer's normal business hours. The Consultant will be accessible via telephone and email. A designated backup will be assigned in appropriate situations. The Consultant will interface with up to two authorized Customer representative(s), who are typically IT or Security personnel responsible for the Customer's UEM production environment. LEVELBLUE will report hours used to provide the Consulting Service on a monthly basis.

The following are not in scope for Consulting Services:

- Consultants will not access or have logon credentials to the Customer's UEM environment. Access will be facilitated by and performed in conjunction with authorized Customer personnel
- Consulting on new mobile OSs or UEM features before they are made generally available
- Consulting on UEM vendors or products not supported by LEVELBLUE or not in production in the Customer's environment
- Installing UEM hardware
- Support or troubleshooting for third party applications
- Documenting of Customer processes or support guides
- Configuring or reconfiguring end user devices for deployment or redeployment
- Customer is responsible for providing the following:
- Access to its UEM environment for the LEVELBLUE Consultant via agreed upon web conferencing.

**LEVELBLUE Business Service  
Guide Omnissa Workspace ONE –**

- Installation of UEM hardware that meets the minimum requirements as published by the UEM vendor and purchase and availability of UEM software.
- Day to day UEM administration, including but not limited to, the following: Device Lock, Wipe, and Passcode Reset; Addition/Deletion of Users and Groups; Device Enrollment; Application of Customer Policies and Profiles; Addition/Updating of Applications and Content; and Reporting.
- UEM technical support, including troubleshooting and resolving end user issues.
- Providing LEVELBLUE up to two technical contacts authorized to interface with the LEVELBLUE Consultant.

**SD-4. Glossary**
*Section Effective Date: 21-Nov-2022*

<b>Glossary</b>	
<b>Acronym</b>	<b>Description/Definition</b>
CRU	Corporate Responsibility User – An Employee receiving service under Customer's account
CSD	Customer Service Desk
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
Help Desk or CSD	Customer Service Desk
IdP	Identity Provider
IRU	Individual Responsibility User – A Customer authorized end user receiving service under an individual account
LDAP	Lightweight Directory Access Protocol
MAM	Mobile Access Management
MDM	Mobile Device Management
MRC	Monthly Recurring Charge
NRC	Non-Recurring Charge
NTP	Network Time Protocol
SCL	Secure Content Locker
SDK	Software Development Kit
SEG	Secure Email Gateway
SLA	Service Level Agreement
SMS	Short Message Service
SSID	Service Set Identifier

<b>Glossary</b>	
<b>Acronym</b>	<b>Description/Definition</b>
SSL	Secure Sockets Layer
SSO	Single Sign-On
TOS	Terms of Service - An agreement between Omnissa and Customer to which LEVELBLUE is not a party and pursuant to which Omnissa assumes all obligations and liabilities to Customer for the items provided thereunder.
UAG	Unified Access Gateway
UEM	Unified Endpoint Management
VCC	Omnissa Cloud Connect
VPN	Virtual Private Network

---

## Country Specific Provisions (CSP)

### CSP-1. General Country Provisions

*Section Effective Date: 05-Dec-2017*

To the extent that Customer or its end users downloads or uses the software on devices in a country other than the U.S., the following additional terms and conditions shall apply:

### CSP-2. Prohibited Countries

*Section Effective Date: 05-Dec-2017*

Device software for the Solution may not be downloaded onto devices by end users who permanently reside in any of the following countries (the "Prohibited Countries"): Cuba, Iran, North Korea, Pakistan, Russia, Sudan, Syria, Turkey, and any countries subject to a US trade embargo at any time.

LEVELBLUE may make changes to the Prohibited Countries from time to time.

#### CSP-2.1. Device and Software Selection

*Section Effective Date: 05-Dec-2017*

Customer is solely responsible for selecting the mobile devices and software/apps (including specifications of associated configuration) that it and its end users may use.

#### CSP-2.2. Data Protection

*Section Effective Date: 05-Dec-2017*

- Customer shall (a) notify, obtain and keep current consents from end users that are required by law for the use or processing of end users' Customer Personal Data, including consents for the transfer to and processing of such data in a country(ies) other than where such individuals are permanently located, (b) give end users the opportunity to opt-in or opt-out to such data transfers and the use of geo-location and cookie functionalities of the Solution; and (c) comply at all times with local language laws to ensure end users have provided informed consent as required by law.
- Customer will only make accessible or provide Customer Personal Data to LEVELBLUE and or its contractors or agents when it has the legal authority to do so.
- Upon not less than thirty (30) days' written notice to Customer, LEVELBLUE may review Customer's practices to implement compliance with this section.

---

**CSP-2.3. Encryption Technology***Section Effective Date: 25-Jun-2020*

Customer represents that it knows and understands the laws governing the cross-border transfer and use of encryption technology, including compliance with trade embargoes, in each country where the Solution will be used. Customer agrees that the duty to comply with laws and regulations governing the importation and use of encryption technology in each country where it uses the Solution - including the requirement to obtain subscriptions and comply with on-going reporting obligations - rests solely and exclusively with Customer.

**CSP-2.4. Filters, Interception and Monitoring***Section Effective Date: 05-Dec-2017*

Customer shall notify and obtain consents from end users for Customer's filtering, interception, and/or monitoring of e-mail and Internet use, and Customer's related processing of Customer Personal Data.

**CSP-2.5. Compliance with Laws***Section Effective Date: 25-Jun-2020*

- Without limiting the generality of any other provision of the Master Agreement between Customer and LEVELBLUE regarding the Parties' respective obligations to comply with applicable law, as between Customer and LEVELBLUE it is Customer's and its affiliates' responsibility to obtain and remain in compliance with the authorizations, subscriptions, consents and permissions required by law for use of the Solution in each country where Customer uses the Solution, and Customer and Customer's affiliates will comply with such laws in respect of their use of the Solution. If and to the extent the applicable laws of any country or portion thereof require information regarding or relating to the Solution to be provided to end users in a language other than English, Customer and Customer's affiliates shall be responsible for providing such information in the required language.
- Upon request by LEVELBLUE, Customer will provide and will ensure that its end users will provide, to LEVELBLUE all assistance reasonably required to enable LEVELBLUE and/or its suppliers to comply with the requests or requirements of any regulator, authority or other competent governmental body in a country where Customer uses the Solution, including in regard to, but not limited to, lawful interception of communications and data retention.

**CSP-2.6. Discontinuance***Section Effective Date: 05-Dec-2017*

LEVELBLUE may discontinue the Solution and/or require Customer and its end users to discontinue the use of the Solution in any country or jurisdiction without liability at any time on thirty (30) days' notice; provided that it may discontinue the Solution immediately if required by a regulatory authority to do so. If LEVELBLUE discontinues the Solution for a reason other than default or breach by Customer, LEVELBLUE will provide a pro rata refund.

**CSP-2.7. Taxes***Section Effective Date: 05-Dec-2017*

LEVELBLUE shall charge and collect taxes based on the delivery of the Solution, software, maintenance, and LEVELBLUE Services to the address provided in the applicable Pricing Schedule or Order form for Customer. For the avoidance of doubt, Customer acknowledges and agrees that it will be responsible for all taxes (including associated interest and penalties) arising from or relating to any distribution or delivery of the Solution software, maintenance, or LEVELBLUE Services by Customer to (or otherwise any use by) any Affiliate or User of Customer.

**CSP-2.8. Additional Indemnification***Section Effective Date: 05-Dec-2017*

To the extent allowed by applicable law, in addition to Customer's indemnity obligations in the Enterprise Agreement, Customer shall defend, indemnify, and hold harmless LEVELBLUE, LEVELBLUE Affiliates, and their respective agents, directors, employees, and officers against any loss, damage, liability, action, demand, or claim arising out of or relating to Customer's failure to comply with any of its duties and/or obligations as set forth in the Country Specific Provisions section, including but not limited to those related to downloads or transmissions of device software in violation of export/import laws and U.S. and multi-lateral trade sanctions.

---

End of Service Guide

*The LEVELBLUE Business Service Guide is subject to change by LEVELBLUE  
from time to time.*

© 2024 LEVELBLUE Intellectual Property. All rights reserved.  
LEVELBLUE, the LEVELBLUE logo and all other LEVELBLUE marks contained herein are  
trademarks of LEVELBLUE Intellectual Property and/or LEVELBLUE affiliated companies.

This document reflects the Service Guide in effect as of September 05, 2024