

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



1. Overview of the Solution

The purpose of this Service Specification is to describe the service that Vodafone provides to its Customers in relation to Vodafone Secure Device Manager (VSDM) Cloud. This Service Specification describes the core functionality, non-functional characteristics, implementation and in-life services that will be provided by Vodafone as part of the VSDM Cloud service.

VSDM Cloud is powered by the Unified Endpoint Management (UEM) software application, Workspace ONE, provided by Omnisia. Vodafone provides the integrated solution and service wrap around the software. The VSDM Cloud solution enables Vodafone Business customers to remotely manage and secure their fleet of Approved Devices, through a range of features including but not limited to: pushing profile policy and security settings to the Approved Device; managing applications on the Approved Device; providing application wrapping of mobile applications and data; controlling access to corporate email and other corporate application servers and providing visibility of the Approved Device estate and the status of Approved Devices. The VSDM Cloud service includes the following core components:

Hardware and Software	Service Set-Up	Service Operation
<ul style="list-style-type: none">• Subscription Licences for VSDM Cloud:<ol style="list-style-type: none">a. Mobile Essentialsb. Desktop Essentialsc. Unified Endpoint Management “UEM” Essentials• Hosting environment of VSDM Cloud (all hardware, operating system, virtualisation and network infrastructure required to present the application functionality to the internet) through Omnisia.• Application software configuration / installation – Optional Service Elements – hosted in Customer’s network, on a Customer provided server<ul style="list-style-type: none">– Omnisia Cloud Connector (CC)– Omnisia Unified Access Gateway– Workspace One Access Portal (console hosted by Omnisia, Workspace One Access Connector hosted by the customer)	<ul style="list-style-type: none">• Solution implementation with Project Coordination• Training services• Operational Manual	<ul style="list-style-type: none">• Help Desk• Application management e.g. patches / upgrades (Omnisia in co-ordination with Vodafone)• Release Management (Omnisia in co-ordination with Vodafone)• Platform Maintenance services (Omnisia in co-ordination with Vodafone)• Incident, problem, capacity and availability management• Service Level Agreement

Table 1. The core and optional components of Vodafone Secure Device Manager Cloud.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



2. Key Functionality of VSDM Cloud

VSDM Cloud is a solution comprised of a Cloud service delivering core functionality that can be complemented by the addition of On Premise Components, extending functionality and adding a layer of security.

VSDM Cloud offers a mix of Workspace ONE packages and add-ons, to allow for a flexible and scalable proposition towards customers, according to their needs, market particularities and stage of their digitalisation journey.

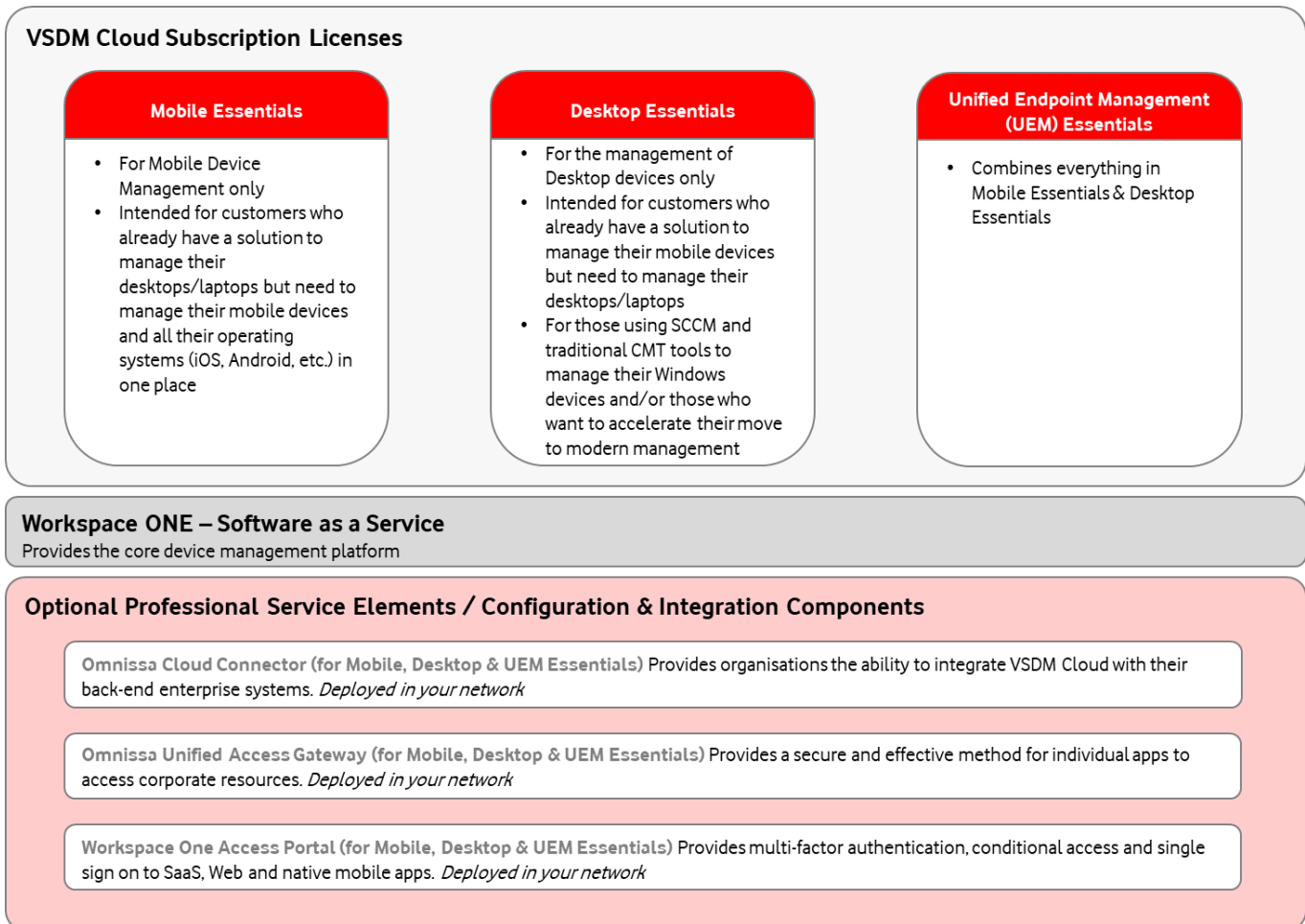


Figure 1. Key functionalities of Vodafone Secure Device Manager Cloud.

With the exception of set-up, training and professional services (see pages 15-17) all licence charges whether core or add-on are monthly in arrears. Please contact your account manager for pricing.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



3. VSDM Cloud Packages and Add-Ons

		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Employee lifecycle experience					
Workspace ONE Intelligent Hub	Securely access apps and company resources, stay connected with colleagues, and be productive from anywhere and on any device with this cross-platform digital workspace application. Personalise for your employees by configuring with the following Hub services.	•	•	•	•
Catalog	Allow 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 categorising applications.	•	•	•	•
People	Allow employees to look up colleagues, view organisation charts, view contact card, initiate calls and emails, and view your team at a glance with the people Hub service.	•	•	•	•
Notifications	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 Omnisia Workspace ONE powered by Boomi can integrate notifications with third- party business systems.	•	•	•	•
Support	Give employees the ability to self-serve with on-demand access to frequently asked questions, knowledge base articles and more as part of the brandable support section in Workspace ONE Intelligent Hub.	•	•	•	•
Branding	Customise the digital workspace experience to reflect your organisation'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.	•	•	•	•
Onboarding	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.	•	•	•	•

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Access services					
Identity broker	Integrate with third-party identity stores and providers, including Active Directory, Azure Active Directory, LDAP, Okta and Ping.	•	•	•	•
Identity provider (IdP) ¹	Serve as the identity database for user accounts. <small>*Functionality limitations for per-device licensing mode.</small>	•	•	•	•
Federated SSO	Federate Active Directory to third-party or internally developed apps using one of the federation standards. Includes a password form-fill feature for SSO.	•	•	•	•
Mobile SSO ¹	Use certificate-based SSO for seamless launching and authentication to iOS and Android apps. On Android, SSO requires Workspace ONE Tunnel. <small>*Functionality limitations for per-device licensing mode.</small>	•	•		•
Multifactor authentication (MFA) ¹	Securely access apps using Verify with Intelligent Hub, FIDO2, TOTP Authenticator Apps, or integrate third-party solutions such as RSA and Duo. <small>*Functionality limitations for per-device licensing mode.</small>	•	•	•	•
Conditional access control ¹	Utilise app access control policy to restrict access to apps based on network ranges, user groups, device platforms, applications and authorisation methods. <small>*Functionality limitations for per-device licensing mode.</small>	•	•	•	•
Workspace ONE Tunnel™	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™.	•	•	•	•
Mobile management					
Mobile device management	Configure mobile device management (MDM) policies, settings and device configurations across phones, tablets and laptop devices that run iOS, Android, macOS, Windows 10 and 11, Chrome OS, Linux and others.	•	•		•
Basic shared device management	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.	•	•		•
Android OEM extensions	Support for OEMConfig—additional OEM-specific device management APIs on top of what's natively available in Android Enterprise (e.g., Samsung Knox, Zebra Managed Configurations).	•	•		•
Mobile app management	Install, track inventory, configure and assign apps—such as internal, public, web and native apps—to users and devices.	•	•		•
App wrapping	Add security policies and management capabilities into an app that is already developed.	•	•		•
Mobile email management	Integrate with email infrastructure to provide access control for ActiveSync clients. Includes support for Office 365, Google Workspace, and Exchange.	•	•		•
Secure Email Gateway (SEG)	Provide access control to the work email server to encrypt data and attachments.	•	•	•	•
Telecom management tools	Track data, call and message consumption, and automate actions and compliance.	•	•		•

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Desktop management					
Modern desktop management	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.	• ²	• ²	•	•
Advanced desktop management	Deliver advanced desktop management capabilities for Windows 10 and 11, 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.			•	•
Enterprise desktop management	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.			• ³	• ³
Workspace ONE AirLift™ for Windows devices	Automate the migration of traditionally high pain-point PC management tasks to Workspace ONE modern management for Windows devices with this server-side connector to Microsoft System Center Configuration Manager (SCCM). Includes capabilities to build and deploy enrollment packages and migrate device collections, GPOs and apps to Workspace ONE.			•	•
IT orchestration framework					
Freestyle Orchestrator	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.		•	•	•
IT compliance automation engine	Build compliance policies with automated remediation workflows, such as app allowlist/denylist, GPS and geofencing, OS version control, and compliance escalation.		•	•	•

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Reporting and automation					
Reports	Utilise reports in the Workspace ONE UEM console.	•	•	•	•
Report customisation and scheduling (snapshot data)	Design custom reports with device, application and user data in Workspace ONE Intelligence.	• ³	• ³	• ³	• ³
Configurable dashboards	Get complete visibility into your digital workspace with rich visualisations at speed and scale.	• ³	• ³	• ³	• ³
Automation engine	Automate processes and take actions with pre-defined rules based on a rich set of parameters. Integrate with third-party tools that support REST API across your environment.	• ³	• ³	• ³	• ³
Device health and lifecycle	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.	• ³	• ³	• ³	• ³
Device health and security	Report on threat and compliance data from sources, including Workspace ONE UEM and Workspace ONE Access™. Automate vulnerability management and OS patching with CVE-based tracking and remediation workflows.	• ³	• ³	• ³	• ³
Mobile productivity apps⁵					
Workspace ONE SDK with DLP protection	Securely integrate mobile apps with Workspace ONE. Includes all modular components of the Workspace ONE SDK, such as app containerisation, security and DLP, SSO, network tunnelling, analytics, privacy and content.	•	•	• ⁶	•
Workspace ONE Boxer	Give employees an all-in-one email, calendar, contacts and files experience via this secure, containerised mobile application, with enhanced security and productivity features built in.	•	•	• ⁶	•
Workspace ONE Notebook™	Help employees manage and compose notes and tasks via this secure, containerised mobile application. Workspace ONE Notebook integrates seamlessly with Exchange, giving users the power to capture, organise, and share thoughts, ideas, meeting notes, images, handwriting and more.	•	•	• ⁶	•
Workspace ONE Web	Give employees frictionless access to intranet sites and web apps via this secure, containerised mobile application. Includes the ability to lock devices into kiosk (single-app) mode.	•	•	• ⁶	•
Workspace ONE Content	Enable employees to aggregate, view and mark up files across on-premises and cloud-based file repositories via this secure, containerised mobile application. Includes mobile content management, file editing and annotation while protecting from data loss with cut/copy/paste/open-in restrictions.	•	•	• ⁶	•
Workspace ONE Send	Enable the secure pass back and forth of Microsoft Intune-protected Word, Excel or PowerPoint attachments between Office 365 apps and Workspace ONE productivity apps.	•	•	• ⁶	•

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Workspace ONE PIV-D Manager	Enable two-factor authentication through a derived credential client certificate via this secure, containerised mobile application that integrates with major derived credential solution providers.	•	•	• ⁶	•
Special purpose device management					
Advanced mission critical device management (Frontline Worker Add-on)	Deliver advanced management for corporate-owned, shared, mission-critical endpoints (e.g., rugged handheld mobile computers and tablets, ruggedised consumer smartphones and tablets in protective cases or sleds, mobile printers, augmented and virtual reality head-mounted wearables, and Raspberry Pi devices). Includes support for Workspace ONE Rugged Enrollment Configuration Wizard (including support for OEM-specific barcode enrollment, such as Zebra StageNow and Honeywell Enterprise Provisioner); advanced shared Android device management with Workspace ONE Launcher™ (including single or multi-app mode, check-in/checkout, and UI customisation); product provisioning; relay servers; and legacy and nontraditional platforms (including Linux, QNX, tvOS, Windows CE, and Windows Mobile).		Add-on		Add-on
Remote support for endpoints					
Workspace ONE Assist for remote support/ management of endpoints	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 CE, Windows Mobile, Windows 10 and 11, macOS and Linux devices.		Add-on	Add-on	Add-on
Experience Analytics with Workspace ONE Intelligence					
Report customisation and scheduling (historical data)	Design custom reports with device, application and user data in Workspace ONE Intelligence.		Add-on ⁴	Add-on ⁴	Add-on ⁴
Device health and lifecycle	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.	• ⁵	• ³	• ³	• ³
Digital Employee Experience Management	Track digital workspace metrics impacting employee experience; proactively identify issues; perform root cause analysis; and quickly remediate across Windows devices, macOS, iOS and Android. Increase employee engagement and productivity.		Add-on ⁴	Add-on ⁴	Add-on ⁴

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



		Mobile Essentials – 30-day Option	Mobile Essentials – 12 & 24 Months	Desktop Essentials	Unified Endpoint Management Essentials
Risk Analytics with Workspace ONE Intelligence					
Report customisation and scheduling (historical data)	Design custom reports with device, application and user data in Workspace ONE Intelligence.		Add-on ⁴	Add-on ⁴	Add-on ⁴
Device health and lifecycle	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.	● ³	● ³	● ³	● ³
Device health and security	Report on threat and compliance data from sources, including Workspace ONE UEM and Workspace ONE Access. Automate vulnerability management and OS patching with CVE-based tracking and remediation workflows.	● ³	● ³	● ³	● ³
Risk-based conditional access with Workspace ONE Intelligence integration	Utilise Workspace ONE Intelligence risk scores in conditional access decisions.		Add-on ⁴	Add-on ⁴	Add-on ⁴
Risk Analytics	Deliver continuous verification based on machine learning with risk analytics and risk scores from device context and user behavior.		Add-on ⁴	Add-on ⁴	Add-on ⁴
Workspace ONE Trust Network	Combine insights from Workspace ONE with integrated security partner solutions—including endpoint detection and response (EDR) solutions, antivirus/malware solutions, mobile threat defense (MTD) solutions, and cloud access security brokers (CASB)—to deliver predictive and automated security in the digital workspace. ⁷		Add-on ⁴	Add-on ⁴	Add-on ⁴
License entitlements					
Default app storage space (for SaaS only)	Utilise the default app storage space. Additional storage may be purchased at 25GB increments.	25GB	25GB	500GB	500GB
Number of licensed devices	Maximum number of devices allowed under management or SDK app managed.	Per-device license: 1	Per-device license: 1	Per-device license: 1	Per-user license: 5
Workspace ONE portal access	Maximum number of devices that may access the Workspace ONE portal through a browser without being managed.	Per-device license: 1	Per-device license: 1	Per-device license: 1	Per-user license: Unlimited

Footnotes to VSDM Cloud Packages and Add-ons Table:

- 1) When licensing Workspace ONE in a device-license model, the SSO, MFA and access control technologies are restricted to only work on licensed devices and from managed apps. Organisations looking to enable access to enterprise apps across devices not licensed for Workspace ONE or allowing access to enterprise apps from any web browser must license Workspace ONE in a per-user license model.
- 2) Workspace ONE Mobile Essentials only supports limited modern desktop management profiles (MDM) for tablet/kiosk use cases (i.e., S Mode/RTM/IoT). Advanced agent-driven PC management capabilities for desktop PCs are not included.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



- 3) Workspace ONE Mobile Essentials includes limited Workspace ONE Intelligence features for mobile device management automation. Workspace ONE Mobile Essentials does not include full Workspace ONE Intelligence capabilities, such as reporting and dashboards with historical data, automations with third-party integrations through custom connectors, Risk Analytics, Digital Employee Experience Management, and Workspace ONE Trust Network.

Workspace ONE Desktop Essentials includes limited Workspace ONE Intelligence features for PC management automation (e.g., patching and CVE automation, compliance with Sensors, etc.). Workspace ONE Desktop Essentials does not include full Workspace ONE Intelligence capabilities, such as reporting and dashboards with historical data, automations with third-party integrations through custom connectors, Risk Analytics, Digital Employee Experience Management, and Workspace ONE Trust Network.

Workspace ONE Unified Endpoint Management Essentials includes limited Workspace ONE Intelligence features for PC and mobile device management automation (e.g., patching and CVE automation, compliance with Sensors, etc.). Workspace ONE Unified Endpoint Management Essentials does not include full Workspace ONE Intelligence capabilities, such as reporting and dashboards with historical data, automations with third-party integrations through custom connectors, Risk Analytics, Digital Employee Experience Management, and Workspace ONE Trust Network.

- 4) With the exception of the Mobile Essentials – 30-day option, the Workspace ONE Assist for remote support, Experience Analytics and Risk Analytics add-ons are available for customers of all Workspace ONE Essentials offerings. Frontline Worker is only available for customers of Workspace ONE Mobile Essentials (except the 30-day option) and UEM Essentials.
- 5) Mobile productivity apps available to all Workspace ONE customers by free download.
- 6) Desktop Essentials customers can download the mobile productivity apps at no additional cost, but Desktop Essentials does not include mobile management features required to secure and manage these apps. For these features, consider Mobile Essentials, or UEM Essentials.

For more information on Workspace ONE, [click here](#).

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



4. User Functionality

To provide immediate User control, and to help reduce calls to the Vodafone UK Care Team, a VSDM Cloud Customer Self-Service Portal is provided, which enables Customer's Users to:

- Self-enrol their device
- Locate their device
- Lock their device

Access to the console is limited to Vodafone Operations and Customer Administrators. Access to the console is based on login credentials. The Customer's Admin will receive a set of credentials and they can set-up access for various other Users, as required. Vodafone Operations will also have access for support and troubleshooting purposes. Vodafone will apply their internal User Access Management (UAM) procedures to manage access to the console. The Customer should apply their own UAM procedures.

5. Technical Overview and Architecture

The VSDM Cloud UEM platform is a fully operational cloud solution that can be activated in a matter of weeks. Additional functionality and integration is achieved by simply installing and configuring the On Premise Components Omnisca Cloud Connector, Omnisca Unified Access Gateway and Omnisca ONE Access Portal.

The solution also includes a number of mobile add-ons for further feature enrichment (some of which come as standard depending on the selected package) including: Advanced mission critical device management (Frontline Worker Add-on), Workspace ONE Assist for remote support/ management of endpoints, Risk Analytics and Experience Analytics.

Architecture

Secure Hosting Platform

The VSDM Cloud platform uses a secure, multi-tenant database architecture, where each customer is configured as a separate Organisational Group – segregated from other customers on the shared SaaS platform. Additionally, Omnisca's hosting environment benefits from advanced security threat management features such as Distributed Denial of Service (DDoS) protection, as well as multiple Intrusion Detection mechanisms.

The VSDM Cloud is centrally hosted in Frankfurt, Germany. This platform is able to provide mobile device management capabilities for devices located anywhere in the world.

Pure SaaS Deployment

The VSDM Cloud solution can be implemented in its most simple form via the VSDM Cloud, where all mobile device management functionality is provided by Omnisca. No Customer premise infrastructure is required with this option. However, this is desirable only when integration with internal corporate systems located within the Customer's network does not form part of the solution.

The features and functions are configured and managed through the VSDM Cloud web console, and the entire solution is delivered from the VSDM Cloud.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers

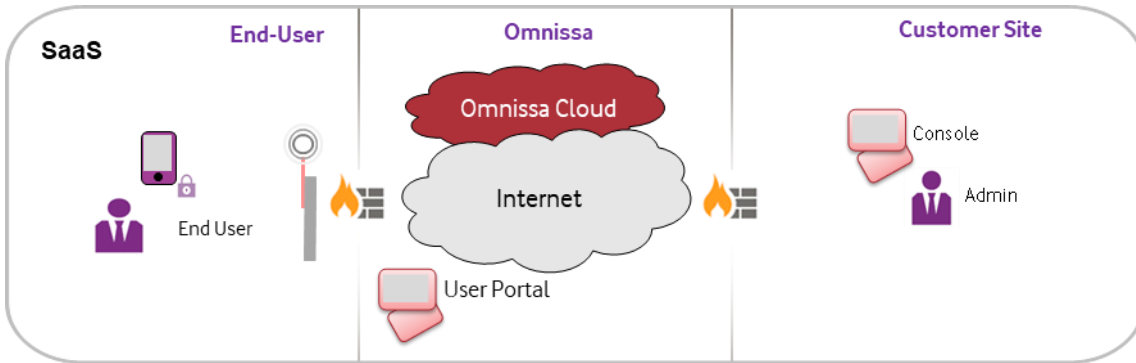


Figure 2. Pure SaaS Deployment with Omnissa.

Integrated SaaS Deployment

To enrich the solution by adding further capability, integration and security, there are optional components that can be installed in Customer's network at a later date should the functionality be required.

- Omnissa Cloud Connector
- Omnissa Unified Access Gateway
- Workspace ONE Access Portal

These act as a seamless integration point for the core device management platform and Customer's services. These are configured through the same console as with a pure SaaS deployment.

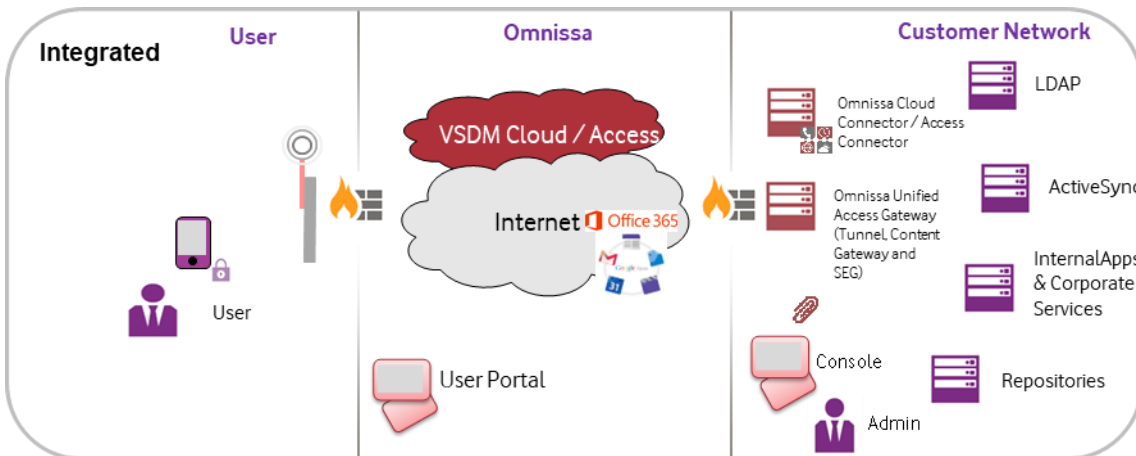


Figure 3. Integrated SaaS Deployment with Omnissa.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



6. Solution Components and Optional Service Elements

Workspace ONE – Software as a Service

The core device management platform is a shared cloud environment that can scale to thousands of customers; Omnissa's platform is built as a multi-tenanted environment with full segregation between individual customer data. This feature also cascades into Customer's defined organisation, such as segregating divisions.

Omnissa Cloud Connector – Optional Component

To leverage the full functional potential of VSDM Cloud, the Omnissa Cloud Connector is available.

The Cloud Connector is a key component for integrating the MDM cloud with internal corporate systems. The most popular use is to integrate with Active directories or LDAP to align the Users of Mobile devices with the corporate mail environment.

The Cloud Connector is hosted within the Customer's internal network (behind the firewall), acting as a proxy allowing VSDM Cloud to integrate with corporate services. This component securely relays requests from the VSDM Cloud to the Customer's critical enterprise infrastructure components.

The Cloud Connector integrates with the following Customer systems and extends the functionality of Mobile Email Management as well as Mobile Application Management:

- Email Relay (SMTP)
- Directory Services (LDAP / AD)
- Microsoft Certificate Services (PKI)
- Simple Certificate Enrolment Protocol (SCEP PKI)
- Email Management MS Exchange (Office 365™ and 2010+)
- Certificate Authority Integration
- Syslog (Event log data)
- Google Mail¹

Note: The Cloud Connector requires a server hosted and managed by the Customer. Additional charges apply for professional services.

Omnissa Unified Access Gateway – Optional Component

The Unified Access Gateway is an additional component deployed inside the Customer's network that enables secure communication between the Users devices and corporate content such as intranet, document repositories (SharePoint), Enterprise applications and MS Exchange.

The Unified Access Gateway acts as a centrally managed entry point for device connectivity to corporate content and data, it is required to leverage the functionality of Workspace ONE Tunnel. Access can automatically be controlled by device, app, and User based on corporate policy.

The Unified Access Gateway authenticates and encrypts traffic from individual applications on compliant mobile devices to the back-end systems they are trying to reach. It allows only selected applications to authenticate and securely communicate with back-end resources.

The UAG extends the capability of Mobile Application Management and Mobile Content Management (part of Workspace ONE Content) by providing secure integration to:

¹ Limited capability if not using Exchange ActiveSync

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



- Internal document repositories and content such as SharePoint and Network Shares (also integrates to Workspace ONE Content).
- Internal websites or web applications using Workspace ONE Web or native browser.
- Secure Email Gateway (SEG) functionality is included as part of the UAG configuration (if required). The SEG is a customer hosted ActiveSync gateway designed to manage and secure mobile device access to corporate email.

Additionally, your employees can use the Unified Access Gateway to access your integrated enterprise applications and services using the per-app VPN functionality provided by the Unified Access Gateway.

By including this component, Customers will have the ability to restrict access automatically based on policies defined by device, app, and User specific properties and state. To illustrate, Customers could restrict a device from accessing Customer's intranet if the device has been "jail-broken" or "rooted".

Note: Additional charges apply for Unified Access Gateway professional services.

Workspace ONE Access Portal – Optional Functionality

Workspace ONE Access (formerly VMware Identity Manager) provides multi-factor authentication, conditional access and single sign on to SaaS, Web and native mobile apps.

Note: Additional charges apply for professional services.

Device Clients

VSDM Cloud uses the Omnisia Intelligent Hub device client to better access functions and manage the devices; it is a requirement that Omnisia Intelligent Hub is installed on the device.

7. Resilience

VSDM Cloud is hosted by Omnisia (Europe - AWS - Germany) and Disaster recovery is also in AWS Germany.

Omnisla Workspace ONE employs a highly available, redundant, and scalable design with Geo-Resilience. Internet access is provided to the Workspace ONE environment via redundant Ethernet connections. Omnisla Workspace ONE is backed by a 99.9% uptime SLA (as defined in the Workspace ONE SLAs).

Omnisla's Information Security Program leverages guidance from industry best practices and regulatory standards, including:

- Omnisla IaaS/hosting providers are ISO 27001 & Soc2 Type II certified
- Omnisla SaaS:
 - Workspace One Intelligence - ISO 27001 & Soc2 Type II certified
 - Workspace One UEM & Access - ISO 27001 & Soc2 Type II certified
- NIST SP 800-53

VSDM Cloud (hosted in Omnisla Cloud) is provided with the following certifications:

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



- TRUSTe
- Safe Harbor
- SSAE 16 (SoC 2) Type II
- FedRAMP
- Workspace ONE UEM Cloud has also achieved the UK Government Information Assurance Framework: Cyber Essentials Plus certification

8. Back-up

The solution has backup and restore functionality and is deployed in a Highly Available (HA) setup with Geo-Resilience.

Redundancy is built into every tier of the infrastructure – from the ISP, to power, to the firewall, routers, load-balancers, and application/DB servers. Customer data is backed up hourly with full nightly backups to a secure offsite location. Backups are encrypted in-transit and at-rest.

Daily backups are stored for 30 days, and support staff review backup processes daily to ensure data integrity.

Workspace ONE application logs are retained for approximately 30 days, (and Omnisca Cloud system audit log data may be kept for 90 days as backups are circulated out of rotation and the data subsequently destroyed).

9. Scalability

VSDM Cloud is designed to support 1 to 100k+ devices and any number of customers.

Any of the optional On Premise Components will be subject to capacity management to meet Customer's requirements.

10. Vodafone Assurance

The VSDM Cloud release roadmap will follow Omnisca releases closely. Prior to deploying any new release as part of VSDM Cloud, Vodafone may conduct additional detailed testing beyond the standard vendor product testing. Vodafone will choose the upgrade date from a range of slots provided by Omnisca.

11. Vodafone Services

VSDM Cloud includes a Help Desk to Help Desk service from the Vodafone UK Care Team. This service is offered as standard and is included in the price of the licence.

Additional services include:

1. VSDM Cloud Set-Up
 - a) Foundation Set-Up (mandatory)
 - b) Advanced (optional)
2. VSDM Cloud Training Service

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



a) Remote

b) Onsite

3. Professional Services

Please contact your account manager for pricing.

12. VSDM Cloud Set-Up Services

The VSDM Cloud set-up service is based on the information completed in the set-up form. If the Customer has opted for advanced set-up, it also requires technical prerequisites that will be discussed as part of a professional engagement call. Engagement with the Customer will take place within 10 working days of receipt of the request.

Customers will need to appoint a technical single point of contact for a joint implementation of the services.

The set-up of the SaaS platform will typically be done within 5 Working Days, however, if training and professional services have been ordered this may take longer dependent on your availability.

The minimum number of VSDM Cloud licenses that can be purchased is 1. Customers will be billed based on the number of licenses ordered. Except for the 30-day Mobile Essentials option, licences are available for a minimum of 12 months.

In order to help you get the most from your investment in VSDM Cloud, Vodafone offers Rapid Adoption Packages as part of Foundation and Advanced set-up.

Foundation Set-Up

Accelerate your MDM journey with guidance from an MDM Specialist. The Standard Rapid Adoption Package is included as part of Foundation Set-Up:

Standard Rapid Adoption Package

- Admin Account Creation and Roles
- User Account Creation
- Android EMM registration
- Apple APNs Certificate
- Profile Creation and Assignment
- Enrolment Methods
- Device Controls
- Application Management

NOTE: The topics covered as part of the Standard Rapid Adoption Package may vary depending on the licence type you have chosen e.g. some licence types have limited functionality and not all items listed above will apply.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



Advanced Set-Up

Advanced set-up requires a professional engagement call with the Customer to assess their requirements and how these will be delivered. These services include the delivery of integration to customer on-premise components (UAG and CC). Pricing is produced as part of the assessment based on customer requirements and is in addition to the foundation set-up costs. Delivery options include on-site or remote.

The Advanced Rapid Adoption Package is included as part of Advanced Set-Up:

Advanced Rapid Adoption Package

- All of the features of the Standard Rapid Adoption Package
- Apple Business Manager Integration (DEP/VPP)
- Samsung Knox Mobile Enrolment
- Active Directory Integration
- Email Management including PowerShell Integration
- Compliance Profiles and Assignment
- Microsoft 365 Integration
- Device Staging
- Multi-user Devices
- Custom Branding of Devices

NOTE: The topics covered as part of the Advanced Rapid Adoption Package may vary depending on your exact requirements.

Roles and Responsibilities

Resource/Role	Key Responsibility
Sales Order Processing Team	VSDM Cloud is available via assisted Sales. The Sales Order Processing Team will submit the order for you on Vodafone Business Marketplace.
Project Co-ordinator	Coordinate installation (Foundation Set-Up/Advanced Set-Up depending on what you have ordered).
UK Onboarding Team	Onboarding into the following systems: <ul style="list-style-type: none">– Help Desk Ticketing Tool– Comms Tool
Endpoint Management & Security Specialist	Initial assessment call with customer to validate their requirements. Install and set-up customer On Premise Components: <ul style="list-style-type: none">– Omnissa Cloud Connector– Omnissa Unified Access Gateway– Workspace ONE Access Portal Remotely or onsite (as ordered).
Training Specialist	Provide remote or onsite training sessions (as ordered).

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



Resource/Role	Key Responsibility
Customer Team	Coordinate all internal activities. Implement the required pre-requisites. Participate in technical sessions with skilled resources. Prepare corporate Apple ID if management of iOS devices is required.

13. VSDM Cloud Training Services

Vodafone provides two offerings:

- 1) Onsite (suitable for 1- 12 people)
- 2) Remote (suitable for 1-12 people)

There is a standard structure for the training courses, but the courses can be tailored to cover the Customer's requirements. Pricing is per session.

14. Vodafone Professional Services

Customers can order additional professional services as part of the solution or as needed during the lifecycle of their service for an additional cost.

Professional Service	Description
Training	Training (both onsite and remote) can be requested at any point during the lifecycle of the Customer's service.
Technical Consultancy	Vodafone offers technical consultancy to: <ul style="list-style-type: none">- Validate the Customer's requirements- Produce a design- Deliver the design (see below) Note: Full documentation of the product is available within the help section of the product so the Customer can complete a self-assessment as required. There are also wizards within the product that help the Customer provision basic functionality.
Installation and Integration Services	Installation of integrating components: <ul style="list-style-type: none">- Omnisca Cloud Connector<ul style="list-style-type: none">o Integration with Email and AD/LDAPo Integration with Certificate Authorities- Omnisca Unified Access Gateway- Workspace ONE Access Portal

15. VSDM Cloud Support Services

As part of the standard product, VSDM Cloud will attract a Support Service as standard.

The Support Service is offered as a Help Desk to Help Desk service in all forms and requires named contacts. Customers can list up to ten contacts responsible for raising Incidents to the Help Desk.

Where reasonably possible, Vodafone will provide these contacts with information about service maintenance, upgrades and releases and for Incidents being work-on.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



NB: Customer's contacts are obliged to cooperate in the resolution of Incidents.

To understand if there are any full or partial outages, it is recommended that Customer Administrators sign up to service status report emails from Ommissa. They will then be able to see the current status of the incident via Ommissa's [Status](#) page.

Incident Management is provided for faults and resolution as described below. The service is offered as standard business hours.

16. VSDM Cloud Support Model

The service is offered as a Help Desk to Help Desk service for up to ten named contacts from the Customer's IT Help Desk.

The named contacts are required to raise platform issues with the Vodafone UK Care Team. Only named contacts can log an Incident. The Vodafone UK Care Team will resolve the Incident with the contact, or escalate the Incident in the first instance internally. If the Incident requires intervention from the vendor, this will be raised to Ommissa for resolution.

17. Service Level Agreement

The Help Desk will apply an SLA to an Incident according to the Category of the service impact.

A full breakdown of Priority Levels and associated Service Levels can be found in your Service Specific Terms.

The Vodafone UK Care Team's opening hours are 8am-6pm Monday to Friday excluding Bank Holidays. P3 and P4 Incidents will only be acted upon during standard business hours. Priority 1 and Priority 2 Incidents will be acted on 24/7. Priority 1 and Priority 2 Incidents only apply to the core device management platform.

18. Platform Support and Maintenance

The underlying technology platform on which the service is based must be effectively managed and maintained in order to deliver the agreed levels of service to Customers. In order to achieve this Vodafone will provide a range of service operation functions as described below.

All Workspace ONE services have achieved ISO 27001/17/18 certification and implement strict controls for data security and monitoring. In addition, Vodafone run an Information Security Management System (ISMS) based on the recommendations of ISO 27001, further details of which can be found in your VSDM Cloud Operational Manual.

Application Management function

A team of dedicated application experts with access to the necessary tools and resources will provide the technical expertise required to manage the application availability and performance and also to request patch and release updates on the application. This includes the activities of application monitoring, health checking and troubleshooting. This team is supported in turn by the application vendor 3rd line support to provide a level of functional escalation in the case of Incidents with the application that cannot be resolved by Vodafone and general bug fixing and patch updates as needed.

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



Scheduled Maintenance

Omnissa schedules pre-defined maintenance windows to limit the potential to impact the environment availability. These standing windows are scheduled annually.

Routine Maintenance

Occasionally, it is necessary for Omnissa to perform maintenance that has the potential to impact the availability of customer environments outside of scheduled maintenance windows, and Omnissa reserve the right to do so. A minimum of 5 days' advance notice is given by Omnissa to Vodafone.

Emergency Maintenance

Emergency maintenance is defined as potentially impactful maintenance activity that must be executed quickly due to an immediate, material threat to the security, performance, or availability of the Service Offering. Omnissa will make every attempt to provide Vodafone with as much advance notice as possible, but notice depends on the severity and critical nature of the Emergency Maintenance.

Omnissa send notification emails on behalf of Vodafone to Customer Administrators advising of upcoming maintenance and any outages.

19. Incident Management

Vodafone will provide an Incident Management process so that in the event of an unplanned outage or other service disruption, normal service can be restored as quickly as possible and the negative impact on the business be minimised. Further information about the Incident Management process can be found in your VSDM Cloud Operational Manual.

20. Customer In-life Obligations

The following Customer obligations apply:

- Provide first line IT Help Desk for Users
- Provide necessary information and relevant technical resource to work with Vodafone to resolve queries
- Ensure Users are running the latest version of the Intelligent Hub (*Previously known as VMware® Agent*)
- Work with Vodafone to coordinate patching and software version updates to integrating components, coordinating for agreed service outages if needed
- Maintain connectivity and reachability or necessary ports/IP/URL relating to the VSDM Cloud SaaS and other required services
- Upon termination, unenroll all devices and delete any organisation groups you may have created in the VSDM Cloud Software. Please refer to the Service Specific Terms for more information about Customer obligations on termination
- Provide User training and documentation if needed
- Completing routine tasks which Customer's is authorised to complete themselves
- Administer the platform - create the policies, configurations, register devices and Users.
- Maintain and amend the policies and configuration as required once the service is live.
- Monitoring any non-Vodafone hosted components (e.g. on site UAG and CC)

Service Specification

Vodafone Secure Device Manager Cloud

Business Customers



Abbreviations

Abbreviation	Meaning
CC	Cloud Connector
CMT	Client Management Tools
IaaS	Infrastructure as a Service
IoT	Internet of Things
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
PKI	Public Key Infrastructure
RTM	Release to Manufacturers
SaaS	Software as a Service
SCCM	Microsoft System Center Configuration Manager
SCEP	Simple Certificate Enrolment Protocol
SDK	Software Development Kit – a set of code and instructions to allow integration of specific features
SEG	Omnissa Secure Email Gateway
SLA	Service Level Agreement – defines what will be done and usually in what timeframes
S Mode	Windows 10 Streamline Mode
Syslog	System Logging Protocol
UAG	Omnissa Unified Access Gateway
UEM	Unified Endpoint Management
VSDM Cloud	Vodafone Secure Device Manager Cloud – Vodafone's branded version of Omnissa's Workspace ONE