VMware Experience Solutions

Workspace ONE Management Modes
Disclaimer

The information in this presentation is for informational purposes only and may not be incorporated into any contract. There is no commitment or obligation to deliver any items presented herein.

The following presentation may contain product features that are currently under development.

This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.

Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.

Technical feasibility and market demand will affect final delivery.

Pricing and packaging for any new technologies or features discussed or presented have not been determined.

This information is confidential.
Agenda

- Introduction
- VMware Anywhere Workspace
- Why Enrollment Matters
- Management Mode Comparison & Terminology Overview
- Management Options by Platform
- Example Use-Cases
- Available Resources
Hybrid Work is Here to Stay

Hybrid Work Model

74%

Companies are using or plan to implement hybrid work model.¹

Diverse Talent Pools

80%

Agree that hybrid work enables organizations to get the most out of diverse talent pools.²

Access to Digital Tools

90%

Say it is on employers to provide the appropriate access to the digital tools to enable remote work.³

¹ US companies only, Source: Future of Work 2022 Hybrid Work Stats, Zippia
² 3. Vanson Bourne, “The Virtual Floorplan” October 2021

² Vanson Bourne, “The Virtual Floorplan” October 2021.
But Challenges Still Remain
Top categories include Experience, Security, and Operational Complexity

- **Sub-optimal Experience**: 80%
  - Agree ability to activate remote workforce as competitive differentiator

- **Fragmented Security**: 64%
  - State that IT security measures implemented have sometimes held back productivity

- **Operational Complexity**: 98%
  - Of organizations anticipate challenges in implementing hybrid work in 2022

1. Distributed Trends, Vanson Bourne 2021
2. The Hybrid Workspace: New Rules for a New Era of Work, September 2021
3. IDC 2022
Legacy Technologies Cannot Scale
Creates Complex Security and Poor Experience

- How can I ensure reliable user experience in remote locations?
- How much do I trust this device?
- How can I efficiently and effectively support remote access?
- How do I restore secure access?
- How do I protect my data?
- Can I support personal devices?
- How can I provide seamless access for enhanced productivity?
VMware Anywhere Workspace
Enabling Customers to Successfully implement Hybrid Work

Outcomes
- Employee Experience
- Workspace Automation
- Zero Trust Security

Workspace Services
- UEM
- VDI DaaS
- Digital Employee Experience
- SaaS App Mgmt.
- Endpoint Protection
- Secure Remote Access
- SaaS/Web Protection

Unified Platform Services
- Unified Admin Console
- End-User Services
- Analytics & Insights
- Workflow & Automation
- Identity & Access Broker
Why Enrollment Method Matters

Enrollment is the **first interaction** between the user and Workspace ONE. It must be simple, easy, secure and delights end-users.

Any **bad experience** can easily spread across the organization by word of mouth and slow down adoption.

A **well-defined** device management strategy is directly correlated to a higher adoption.

Provide users **clearly-defined** terms of use, transparency and communication.
Management Mode Terminology and Comparison
Management Mode Terminology
What does it all mean?

Workspace ONE Terminology

- **UEM Managed**
  - MDM Managed
  - Fully Managed Personal (BYOD) and Corporate devices
  - Device managed by a single MDM only

- **OS Partitioned**
  - Android Work Profile
  - iOS User Enrollment
  - Managed “Side”
    - Personal (BYOD) and Corporate devices
    - Device can be ONLY managed by single MDM

- **Hub Registered**
  - Managed “Side”
    - Personal (BYOD) and Corporate devices
    - Device can be ONLY managed by single MDM

- **App Level**
  - Unmanaged
  - MAM Mode | Standalone
    - Mode | Unmanaged
    - Management limited to apps, versus device-level management
      - Personal (BYOD) devices
        - Device can be managed by third-party MDM when Workspace ONE UEM is managing the apps
## Management Mode Comparison

### Overview

<table>
<thead>
<tr>
<th>Mode</th>
<th>macOS</th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UEM Managed</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device is fully managed by UEM admin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Push commands, configurations, policies and applications to the device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Intelligent Hub and MDM Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OS Partitioned</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management restricted to only business applications and business data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No personal information can be accessed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enrollment starts by installing the Workspace ONE Intelligent Hub app from the store</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Intelligent Hub and MDM Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hub Registered Mode</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management is limited to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• enforce policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• wipe corporate app data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exception for Windows 10:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Administrator can apply device baselines and collect device information through sensors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Intelligent Hub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Administrator can't push apps to the device, user must request through Hub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No MDM Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>App Level (MAM)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management restricted to Workspace ONE SDK apps, such as:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Workspace ONE Web</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Workspace ONE Boxer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Workspace ONE Content</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device registration starts with the SDK-based app</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intelligent Hub not required for Workspace ONE productivity apps:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• However, no catalog, people search, notifications, etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No MDM Profile</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Workspace ONE UEM Console

List of enrolled devices with management mode and compliance status

<table>
<thead>
<tr>
<th>Device ID</th>
<th>General Info</th>
<th>Platform</th>
<th>User</th>
<th>Enrollment</th>
<th>Compliance Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>molver</td>
<td>VMware7.1 Windows Desktop 10.0.19...</td>
<td>Windows Desktop VMware7.1 10.0.19042</td>
<td><a href="mailto:molver@airlab.com">molver@airlab.com</a></td>
<td>Enrolled</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / Field Contractors Hub Registered</td>
<td></td>
<td>molver</td>
<td>Mary Oliver</td>
<td></td>
</tr>
<tr>
<td>ilopez</td>
<td>VMware Virtual Platform Windows Desk...</td>
<td>Windows Desktop VMware Virtual Platform 10.0.19042</td>
<td><a href="mailto:ilopez@airlab.com">ilopez@airlab.com</a></td>
<td>Enrolled</td>
<td>Compliant</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / Corporate Headquarter (HQ) UEM Managed</td>
<td></td>
<td>ilopez</td>
<td>Linda Lopez</td>
<td></td>
</tr>
<tr>
<td>Alanusse</td>
<td>Desktop Windows Desktop 10.0.19...</td>
<td>Windows Desktop VMware7.1 10.0.19042</td>
<td><a href="mailto:alanusse@airlab.com">alanusse@airlab.com</a></td>
<td>Enrolled</td>
<td>Compliant</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / Corporate Headquarter (HQ) UEM Managed</td>
<td></td>
<td>Alanusse</td>
<td>Andreano Lanusse</td>
<td></td>
</tr>
<tr>
<td>Alanusse</td>
<td>Desktop Windows Desktop 10.0.19...</td>
<td>Windows Desktop XPS 13 9360 10.0.19042</td>
<td><a href="mailto:alanusse@airlab.com">alanusse@airlab.com</a></td>
<td>Enrolled</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / Field Contractors Hub Registered</td>
<td></td>
<td>Alanusse</td>
<td>Andreano Lanusse</td>
<td></td>
</tr>
<tr>
<td>Alanusse</td>
<td>iPad iOS 14.4.0</td>
<td>Apple iOS 14.4.0</td>
<td><a href="mailto:alanusse@airlab.com">alanusse@airlab.com</a></td>
<td>Enrolled</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / Field Contractors App Level</td>
<td></td>
<td>Alanusse</td>
<td>Andreano Lanusse</td>
<td></td>
</tr>
<tr>
<td>mli</td>
<td>Android 9.0.0 CWSY</td>
<td>Android samsung SM-G950U1 9.0.0</td>
<td><a href="mailto:mli@airlab.com">mli@airlab.com</a></td>
<td>Enrolled</td>
<td>Not Available</td>
</tr>
<tr>
<td></td>
<td>ACME Corp / BYOD UEM Managed</td>
<td></td>
<td>mli</td>
<td>Michael Li</td>
<td></td>
</tr>
</tbody>
</table>
Workspace ONE UEM Console

Device information and actions limited based on the enrollment method

**UEM Managed**
- **Device: Alanusse Desktop Windows Desktop 10.0.19...
  - VMware UEM: Yes, Profile: Alanusse Lunesa

**Hub Registered**
- **Device: moliver Desktop Windows Desktop 10.0.19...
  - VMware UEM: Yes, Profile: moliver
Enable Intelligent Hub Registered Mode

Groups & Settings

Manage advanced console-wide settings:

- **Groups**
  Create and manage custom named groups for specific needs.

- **All Settings**
  Setup, installation, Console settings, and other advanced configuration options.

- **Configurations**
  Establish the foundational settings, customizations, and integrations to provide employees with the resources they need to drive your business forward.
Management Options by Platform
Mobile Management Options Overview

Along the Gradient

- **More Admin Control**
  - Full Device Management
  - OS Partitioned
  - Hub Registered Mode
  - App Level Management

- **More User Privacy**

[Containerized Apps]

[Corp-Owned | BYOD]
Android Management Options
Along the Gradient

More Admin Control →

- Work Managed (aka Device Owner Mode)
- Corporate Owned Personally Enabled (COPE)
- Knox for Play = Work Profile + Samsung Knox
- Work Profile Mode
- Hub Registered Mode (Intelligent Hub Registered)
- App Level Management

More User Privacy →

Corporated Apps

Corp-Owned   BYOD

Containerized Apps
iOS Management Options
Along the Gradient

More Admin Control

- Apple Business Manager or Apple School Manager (Automated Device Enrollment) + Supervised
- Supervised Device Enrollment
- Unsupervised Device Enrollment
- iOS User Enrollment
- Hub Registered Mode (Intelligent Hub Registered)

More User Privacy

- App Level Management

Containerized Apps

Corp-Owned
BYOD
**Lighter Touch Management Option: OS Partitioned**

Provide user app access without full device management

<table>
<thead>
<tr>
<th>iOS User Enrollment</th>
<th>Android Enterprise Work Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Lite&quot; enrollment for iOS 13+ and iPadOS 13+</td>
<td>Separates corporate and personal data on the device</td>
</tr>
<tr>
<td>Establishes managed identity on the device</td>
<td>Ability to enterprise wipe all work data</td>
</tr>
<tr>
<td>Separates data for Mail, Contacts, Calendar, Files and Keychain</td>
<td>Adsms have limited controls compared to MDM enrollment</td>
</tr>
<tr>
<td>Ability to enterprise wipe all work data</td>
<td></td>
</tr>
</tbody>
</table>
Android Enterprise Work Profile

End user experience
macOS Management Options
Along the Gradient

More Admin Control

Apple Business Manager or Apple School Manager (Automated Device Enrollment) + Supervised

User-Approved Device Enrollment

Device Enrollment (via automation or scripting)

User Enrollment (On Roadmap)

More User Privacy

Intelligent Hub via Browser (access apps, VDI)

Corp-Owned  BYOD
Windows 10 Management Options
Along the Gradient

More Admin Control

MDM Enrolled (via multiple onboarding methods)

Hub Registered Mode (Intelligent Hub Registered)

Intelligent Hub via Browser (access apps, VDI)

More User Privacy
When Do I Use Each Management Mode?

Example Use Cases
"I just need email access on my phone."
Entry-level use case

<table>
<thead>
<tr>
<th>Contract Employee, BYOD, Temp Worker, frontline worker, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace ONE Intelligent Hub not installed</td>
</tr>
<tr>
<td>Stand-alone Workspace ONE Boxer email client</td>
</tr>
<tr>
<td>App Level management mode</td>
</tr>
</tbody>
</table>
"I just need email access on my phone."

App Level Management – UEM Console View
"Contractors need access to internal web applications."

OPTION 1 – Workspace ONE Web

Enrollment through Workspace ONE Web

App Level Management

No App Catalog

Only bookmarks in Web app

DLP on the Web App
"Contractors need access to internal web applications."

OPTION 2 – Intelligent Hub (Registered Mode) with Workspace ONE Web

- **Registered Mode**
  - **Intelligent Hub**
  - **App Catalog and Web Clips**
  - **Install native mobile apps from the catalog**
  - **Federated Apps integrated to launch through Web, requires Workspace ONE Access**
  - **Better User Experience**
"I need access to corporate Wi-Fi in several offices."

Any Device Platform

- Users and Devices
  - Cert-Auth

- Workspace ONE UEM (SaaS)
  - Outbound Only 443

- AirWatch Cloud Connectors
- Certificate Authority

**On-Premises**

- UEM Managed required
- Must authenticate device
- Certificate auth for Wi-Fi, eliminating password entry
- Can be extended to email, web applications, etc.
"I need access to internal applications, SaaS and VDI."

Any remote workers
Hub Unified Catalog
- Deploy Native Apps
- SaaS, Web, Internal, VDI

Conditional Access (Device Compliance + User Risk Score) to determine access to applications – requires UEM managed
"Apply Zero Trust principals to determine application access"

Secure access to Web, SaaS, Virtual Desktops and Published Applications

1. HTTPS
2a. Authentication
2b. Risk Score
2c. MFA
3. SAML Assertion

Unified Access Gateway

DMZ or Cloud Tenant

Internal Resources

Web Applications
Virtual Desktops and RDSH Apps

SaaS Apps

Workspace ONE

Access

Workspace ONE Intelligence

Office 365
salesforce
zoom
workday

Workspace ONE

Access

Web
Applications

Workspace ONE

Intelligence

SaaS Apps

Virtual Desktops
and RDSH Apps
Risk Score Aggregation
Compute a personalized Risk Score for every device and user in an organization

Are there unknown, rare or questionable apps?
“The user tends to accumulate apps and not consider their reputation”

Is the device’s OS up-to-date?
“The user systematically ignores or keeps delaying software update”

Are device security capabilities enabled?
“The device is missing a critical patch”

John’s devices

Android Device Score
Low

iPad Device Score
Medium

macOS Device Score
Medium

Windows 10 Device Score
High

User Risk Score
Low Medium High

John Doe
## Summary

### General guidelines

<table>
<thead>
<tr>
<th>UEM Managed</th>
<th>OS Partitioned</th>
<th>Hub Registered Mode</th>
<th>App Level (MAM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>macOS, iOS, android</td>
<td>macOS, iOS, android</td>
<td>macOS, iOS, android</td>
<td>iOS, android</td>
</tr>
</tbody>
</table>

**Provide access to corporate resources and fully manage the device**

**Use Cases:**
- Corporate Dedicated
- Corporate Shared
- Personal device (BYOD)

**Device is fully managed by UEM admin**

**Push commands, configurations, policies and applications to the device**

**Requires Intelligent Hub and MDM Profile**

---

**Provide access to corporate resources and manage the business side of the device**

**Use Cases:**
- Personal device (BYOD)
- Corporate Dedicated

**Push commands, configurations, policies and applications for work data only**

**Requires Intelligent Hub and MDM Profile**

---

**The user can access the catalog of corporate applications without full management of the device**

**Desktops**

IT can enforce baselines on Windows 10 and use sensors to collect additional device info.

**Use Cases:**
- End-user requires access to corporate resources from personal device without giving IT full control of the device

---

**Allow organizations to provide access to corporates resource on a per-app bases**

**Use Cases:**
- Employee needs access to email only without providing IT management of the device
- Contractors needs access to internal websites from personal devices, and IT needs to apply security policies only to the corporate app
Ready to Learn More?
https://euc.techzone.vmware.com/

TECH ZONE CONTENT

• A New Species: Remote Worker

• Enabling Registered Mode for Windows 10 and DEEM

• Steps to Enable a Remote Workforce with Workspace ONE - Part 1 | Part 2

• DEX Solution Overview | DEX Solution Architecture

• VMware Workspace ONE and Horizon Reference Architecture

• How to Enable Intelligent Hub without Full Management

• Mastering Workspace ONE

• Onboarding Options for macOS
## Resources to Get You Started
We have you covered whether you are learning, testing, or ready to deploy...

<table>
<thead>
<tr>
<th>Learn More About Workspace ONE UEM</th>
<th>Test Drive Workspace ONE UEM on Your Devices</th>
<th>Start Your UEM PoC or Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Workspace ONE Hands on Labs" /></td>
<td><img src="image2.png" alt="Workspace ONE on TestDrive" /></td>
<td><img src="image3.png" alt="Workspace ONE Operational Tutorials" /></td>
</tr>
</tbody>
</table>

- Workspace ONE Hands on Labs
- Workspace ONE on TestDrive
- Workspace ONE Operational Tutorials
Thank You