DOCUMENT – JULY 2021

PRINTED 26 MAY 2022

WHAT IS WORKSPACE ONE?

VMwareWorkspace ONE

vmware

Table of Contents

What Is Workspace ONE?

VMware Workspace ONE® is a digital platform that delivers and manages any app on any device by integrating access control, application management, and unified endpoint management. The platform allows IT to deliver a digital workspace that includes the devices and apps of the business's choice, without sacrificing the security and control that IT professionals need. Take a look at this introductory demo to learn how Workspace ONE can help you.

Now that you have a high-level overview of what Workspace ONE can do for you and your organization, this article will help you understand the key features and architecture.

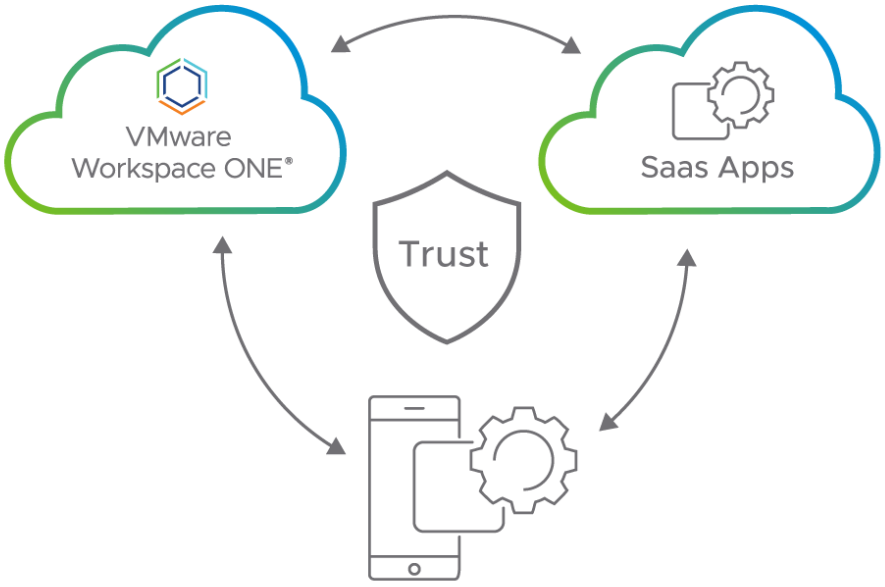
What are the key features of VMware Workspace ONE?

Today's end-users have multiple devices of various forms and operating systems. Many of these devices are not managed by IT, which makes it difficult to secure access when you cannot trust the device. In addition, you have a wide variety of apps that you have to support such as legacy apps, modern apps (SaaS, native, mobile, etc.) and virtualized applications. IT must adapt to changing business needs of the business and embrace the new way of work. That is where Workspace ONE comes in, with the capabilities to meet these challenges.

This section summarizes the key features of Workspace ONE and outlines a few key examples and use cases of when you would use each one.

Consumer-simple app authentication

With Workspace ONE, end-users can get password-less single sign-on to a catalog that provides them access to virtually any app. This includes mobile apps, web apps, cloud apps, and Windows apps. Once signed-in, end-users can self-service select the applications they need to be productive with no IT intervention. As an IT professional, you control the back-end workflow to provide an excellent user experience that doesn't sacrifice security.



- Provide easy access to all the apps your end users need to do their job - either through the Workspace ONE Intelligent Hub or with the browser-based catalog.
- Transform employee onboarding by enabling self-service access to the apps your end-users need.
- One-touch single sign-on means your end-users don't have to remember a bunch of credentials or type in the same password every time they access an app. Workspace ONE uses certificates to establish trust, providing a password-less,

single sign-on (SSO) experience.

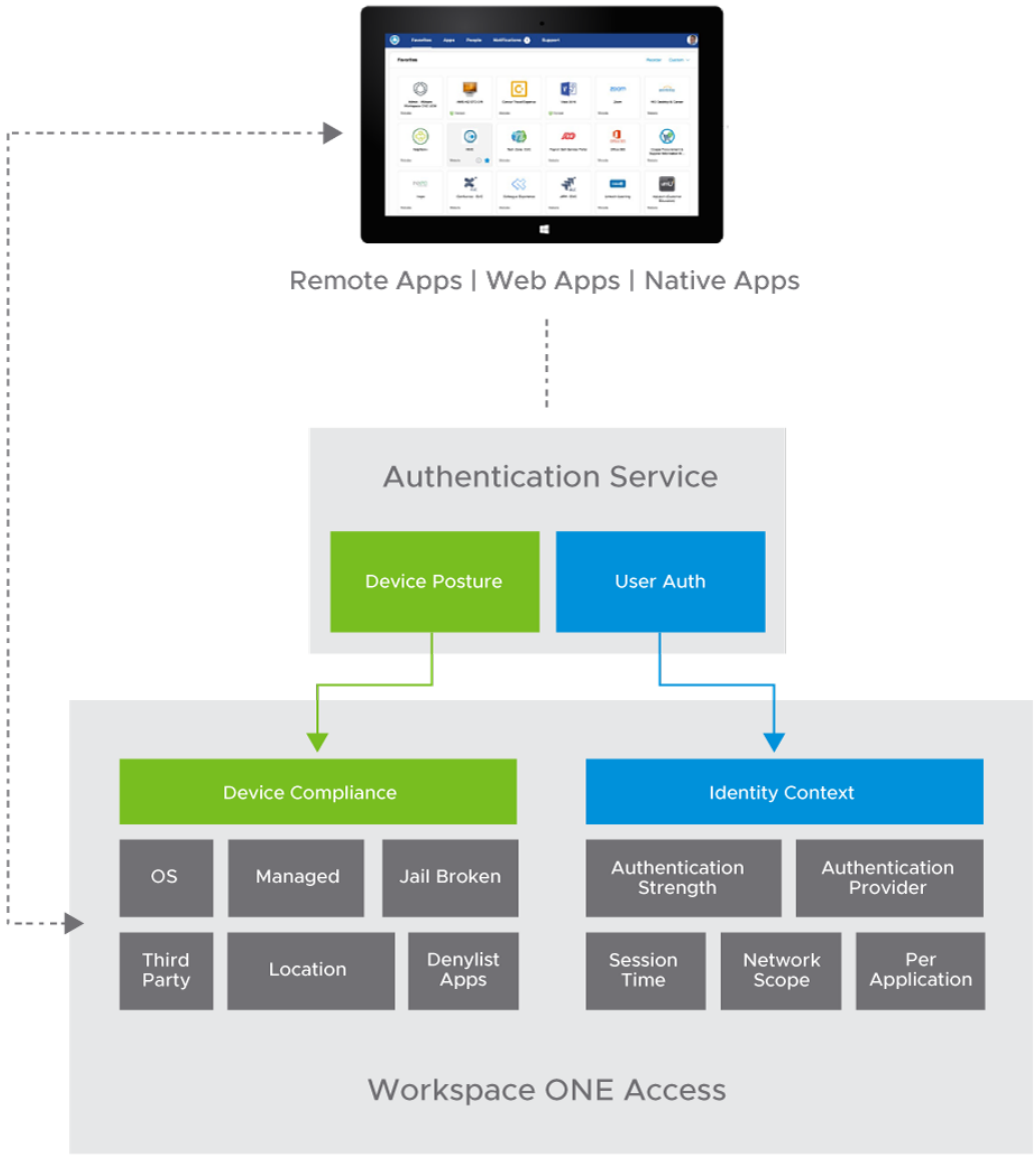
Unified Endpoint Management options

Workspace ONE doesn’t dictate which platforms to deploy in your environment. Our goal is to support any device - even devices that have not yet been invented. From desktop OS’s to mobile OS’s, even wearables, and 3D graphics workstations, we work with it. Beyond that, we also know that while some devices are corporate-owned and require IT management throughout their lifecycle, many will be owned by the employees themselves. Workspace ONE puts the choice in employees’ hands for the level of convenience, access, security, and management that makes sense for their work style.

- Desktop OS's, mobile OS's, smartphones, you name it, we support it. That means you don’t have to worry about the next big mobile device that comes out. We will support it.
- Bring-your-own, Choose-your-own, Corporate Owned, Locked Down, and so on…there are so many device management types. Workspace ONE supports them all in a single platform.
- The Workspace ONE Intelligent Hub makes logging in on a BYO device super simple for end users. From the hub, they can seamlessly launch apps. However, if they try to access an app with confidential data, they are prompted to elevate management on their device.

Conditional access

To protect the most sensitive information, Workspace ONE enforces access decisions based on device compliance and identity context. Using our powerful policy engine, you can mix and match inputs to make dynamic decisions on the level of access end-



users get.

This means, if you need to keep remote users on unmanaged devices from accessing data, you can make that happen with a few clicks. But Workspace ONE doesn't just deny access. We take things one step further and help end-users reach compliance. This keeps your data secure while granting end-users the access they need.

- Apply conditional access policies on a per-application basis to enforce authentication strength and restrict access by network scope, location, and device compliance.
- Provide a range of advanced device restrictions and policies such as: data leak protection against rooted or jailbroken devices, allowlist and denylist for apps, open-in app restrictions, cut/copy/paste restrictions, geofencing, and network configuration.
- Get real-time visibility with application, device and console events that provide detailed information for system monitoring, and view logs in the console or export pre-defined reports.

Automated app management

Workspace ONE allows IT professionals to automate application distribution and updates on the fly. Whether you're deploying Windows apps or mobile apps, we automate the application delivery process to allow better security and compliance. With

Workspace ONE you can deploy Windows apps to Windows 10 devices in your organization or up-to-date apps to mobile devices, from a single platform that keeps you covered every step of the way.

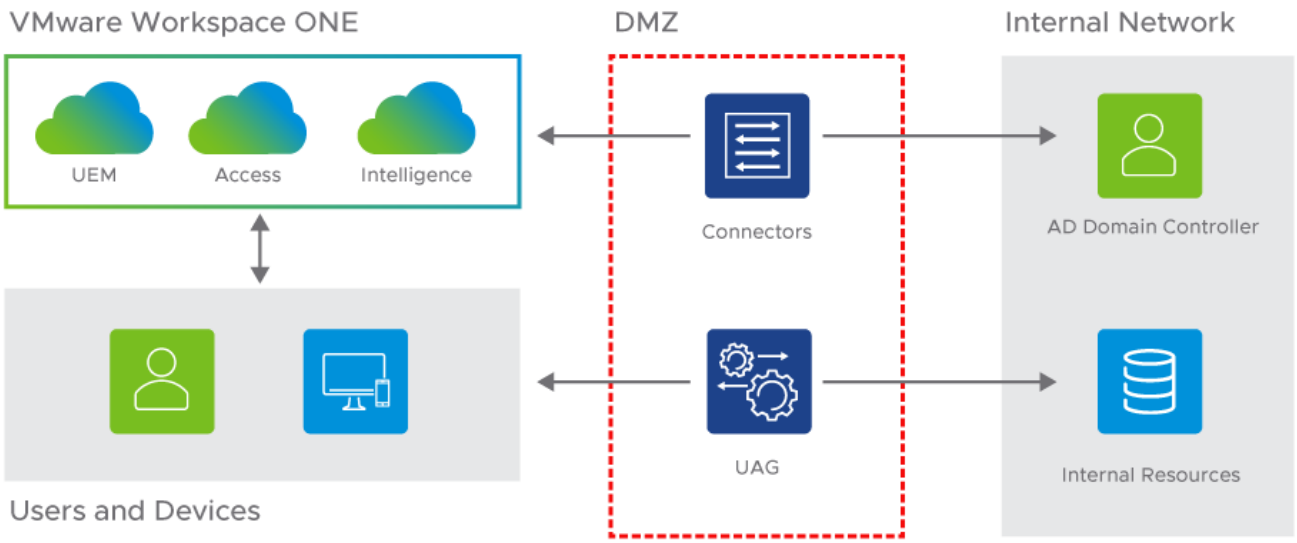
- Eliminate the need for laptop imaging with Workspace ONE's simplified device management and provisioning. Our dynamic smart groups, which use device information and user attributes, ensure devices always have necessary configurations such as Wi-Fi and VPN.
- Automatically install, update, and remove software packages. Create an automated workflow for software, applications, files, scripts, and commands to install on laptops. Configure installation based on a variety of IT-defined conditions.
- Secure hosted virtual apps and desktops enabling users to work on highly sensitive and confidential information without compromising security with Horizon. Users can access their virtual apps and desktops from the Workspace ONE Intelligent Hub app, enabling the flexibility to be productive wherever they are.

What is the architecture of Workspace ONE?

IT can deploy VMware Workspace ONE in a variety of deployment models, including on-premises, in the cloud, and hybrid with different components deployed on-premises and in the cloud.

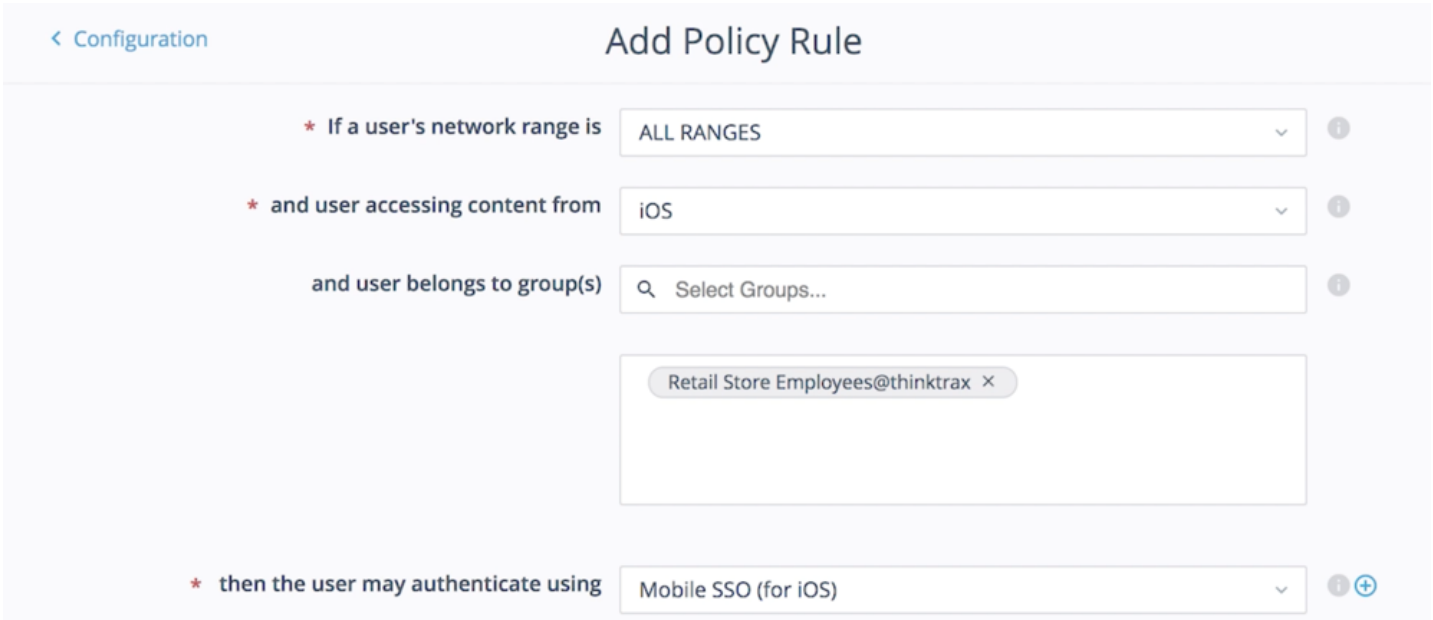
Since the purpose of Workspace ONE is to manage secure application delivery to your end-users, it's critical that you connect Workspace ONE to an existing directory infrastructure. You can configure Workspace ONE to use Active Directory or other LDAP-based directories, for user synchronization, authentication, and application access.

For the sake of simplicity, we're going to focus this article on a basic cloud deployment of Workspace ONE. The larger your environment, the more complex the requirements get, so we can't walk through every detail here. This article is intended just to give you the info you need to understand how some of the elements would fit into your environment at a high level. We can split the architecture into infrastructure and end-user components.

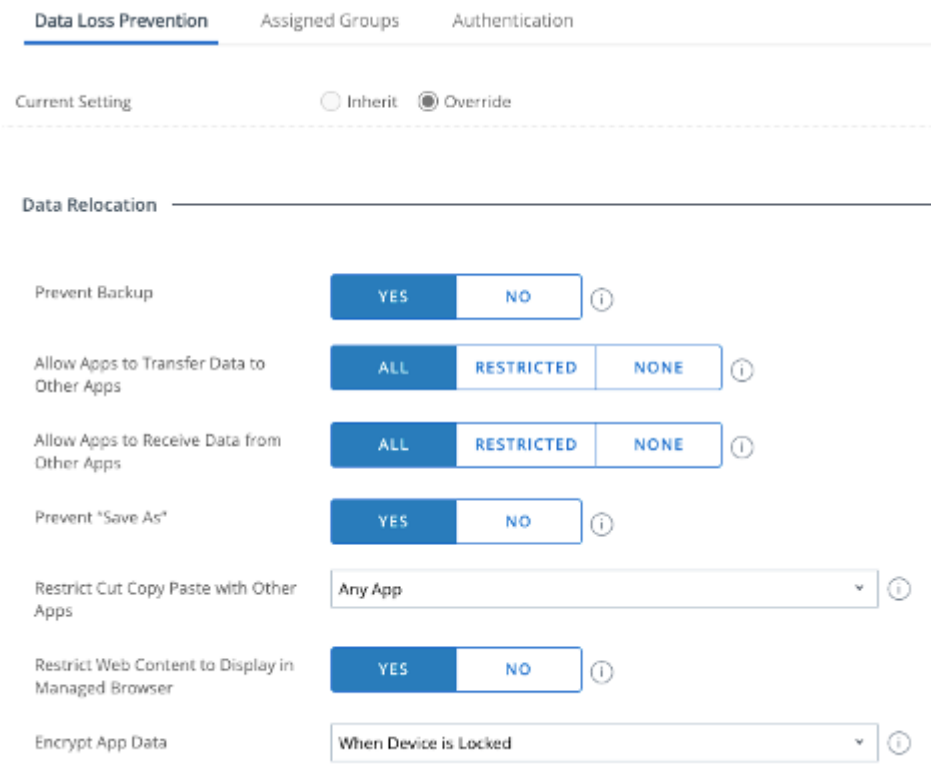


Workspace ONE components

- **Workspace ONE Access** (formerly known as VMware Identity Manager) provides SSO to an application store for software-as-a-service (SaaS)-based Horizon, Citrix, VMware ThinApp®, and web applications, as well as for Horizon virtual desktops. It also provides a set of networking and authentication policies to control application access. For example, in the following screenshot, we can create detailed rules specifying specific authentication rules based on network range, what device the request is coming from, and the Active Directory group.



- **Workspace ONE UEM** (formerly known as AirWatch) provides a comprehensive enterprise mobility platform that delivers simplified access to enterprise applications, secures corporate data, and allows mobile productivity. It also works with the public application stores, to handle the provisioning of native mobile applications to mobile devices. Workspace ONE UEM provides compliance-checking tools to ensure that remote access devices meet corporate security standards. For Office 365, and our integration with the Office 365 Graph API we can manage the DLP settings across the suite of Office applications to ensure security.



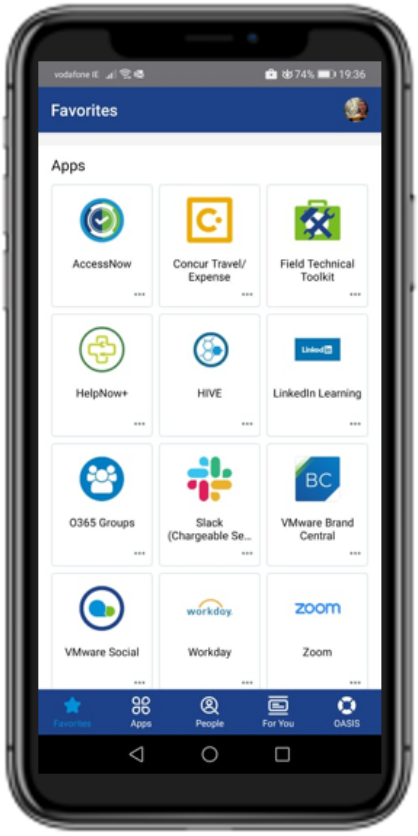
For Windows 10 and other devices, Workspace ONE UEM can apply device profiles that allow you to configure security settings that will keep devices secure (encryption, Windows Updates, and so on), but also some features that will really improve the experience for end users (configuring Wi-Fi and VPN for example).

- **VMware Workspace ONE® Intelligence™** is a cloud-only service, hosted on Amazon Web Services (AWS), designed to simplify user experience without compromising security. The intelligence service aggregates and correlates data from

multiple sources to give complete visibility into the entire environment. It produces the insights and data that will allow you to make the right decisions for your VMware Workspace ONE deployment. Workspace ONE Intelligence has a built-in automation engine that can create rules to take automatic action on security issues.

- **VMware Unified Access Gateway** is a platform that provides secure edge services and access to defined resources that reside in the internal network. This allows authorized, external users to access internally located resources in a secure manner.

Workspace ONE Intelligent Hub



The primary end-user component is the Workspace ONE Intelligent Hub application. The Intelligent Hub app allows end users to access enterprise and Web apps, stay connected with colleagues, and be productive on any device (Android, iOS, macOS, Windows 10) from anywhere.

For a corporate-owned device, the Intelligent Hub app can be set to install automatically after device enrollment. Or, for personal devices, end users can manually install the app from https://getwsone.com. Once installed, end-users will log in with their Active Directory credentials and see the applications that IT has allowed access to. From a single app, end users can view favorite apps, new apps, recommended apps, and categories all within the Intelligent Hub catalog.

Some applications are marked with Requires VMware Tunnel. Tunnel sets up a VPN connection and connects corporate apps to corporate resources. For applications that contain sensitive data, enrolling in management is the way to go, since it provides greater security including encryption, data protection, compliance, and removing enterprise applications when a device gets unenrolled.

End-users also get the benefit of mobile SSO, or as some call it, password-less authentication. For iOS, a Kerberos certificate is passed down to the end-user device. Users who are successfully signed in to their domain can access their Intelligent Hub catalog apps without additional credential prompts. It's really a win-win for IT and end-users.

Top 5 things you should know

Now that you've established a solid foundation of what Workspace ONE can do for you, hear directly from VMware product experts about the top 5 things you should know about Workspace ONE. This tech talk will help you understand how key product features in Workspace ONE will work for you.

Learn more about Workspace ONE

The fastest way to learn Workspace ONE is to check out the Mastering Workspace ONE activity path. On this activity path, you'll find a curated set of articles, videos, and labs to help you level up your Workspace ONE knowledge.

Additionally, check out the Workspace ONE Frequently Asked Questions (FAQs) which provides answers to some of our most popular Workspace ONE FAQs.

Learn more about other VMware projects

If you are interested in other VMware projects, see the following introductions:

- What Is VMware Workspace ONE UEM?
- What Is VMware Horizon?
- What is VMware Dynamic Environment Manager?

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com