REVISED 1 MAY 2018

WHAT IS WORKSPACE ONE?

vmware®

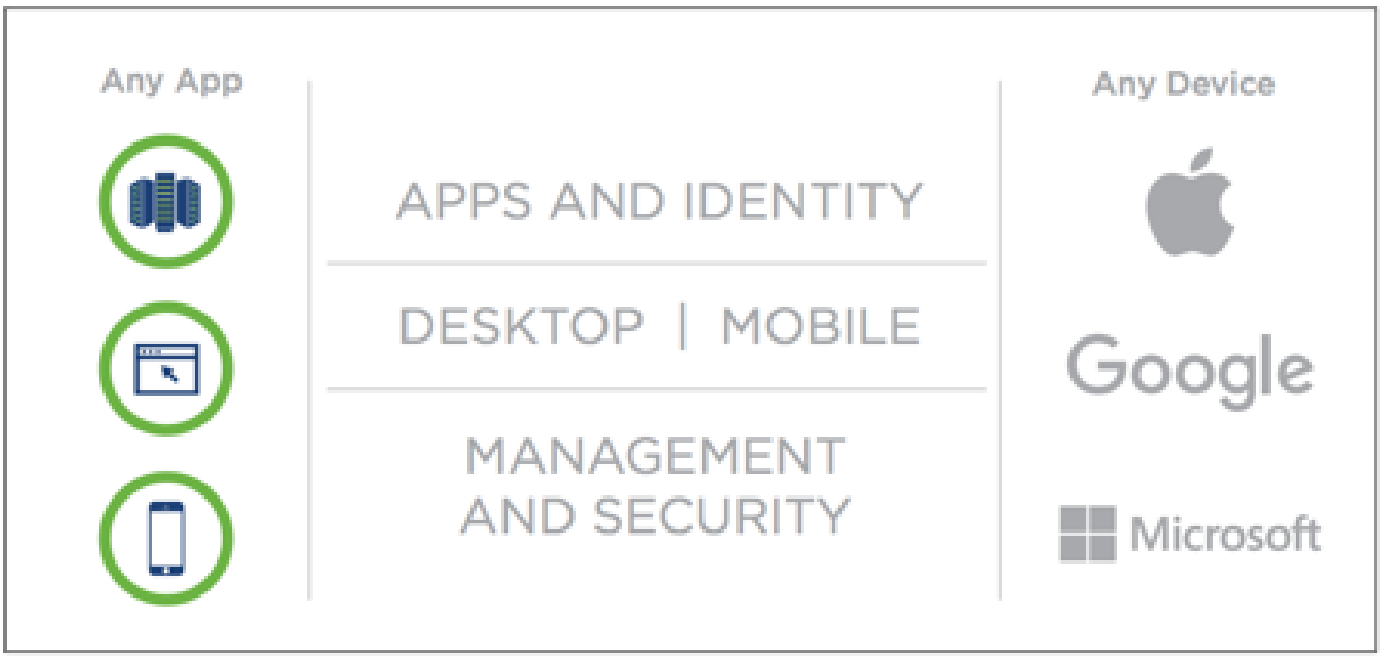
Table of Contents

What Is Workspace ONE?

Compared to other VMware End User Computing products such as Workspace ONE Unified Endpoint Management™ (UEM) powered by AirWatch® and VMware Horizon®, Workspace ONE seems relatively new. However, before you start thinking about Workspace ONE as a brand new product offering, you should know that many customers are already using some of the components that make up the VMware Workspace ONE platform.

So, what is VMware Workspace ONE?

VMware Workspace ONE is VMware's workspace solution. It's a digital platform that delivers and manages any app on any device by integrating access control, application management, and multi-platform endpoint management. Workspace ONE is built on the unified endpoint management (Workspace ONE UEM, formerly known as AirWatch) technology and integrates with virtual application delivery (VMware Horizon) on a common identity framework. The platform enables 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.



VMware Workspace ONE delivers on critical needs that organizations are having today and will have in the future. Think about it. Today, end-users have multiple devices, with various form factors 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. Think about the apps you have to support today. In addition to the legacy apps that you've supported for the last 10+ years, you have modern apps (SaaS, mobile, etc) that sit in the cloud somewhere, outside the realm of the corporate network.

IT has struggled to keep up with the needs of the business and because of that, we see many business units and employees going around IT policy, a trend commonly known as "shadow IT". Organizations are facing the critical decision to either ignore these trends at the peril of unintended security breaches or embrace the new way of work leveraging a new management framework. That is why in 2016 we introduced VMware Workspace ONE.

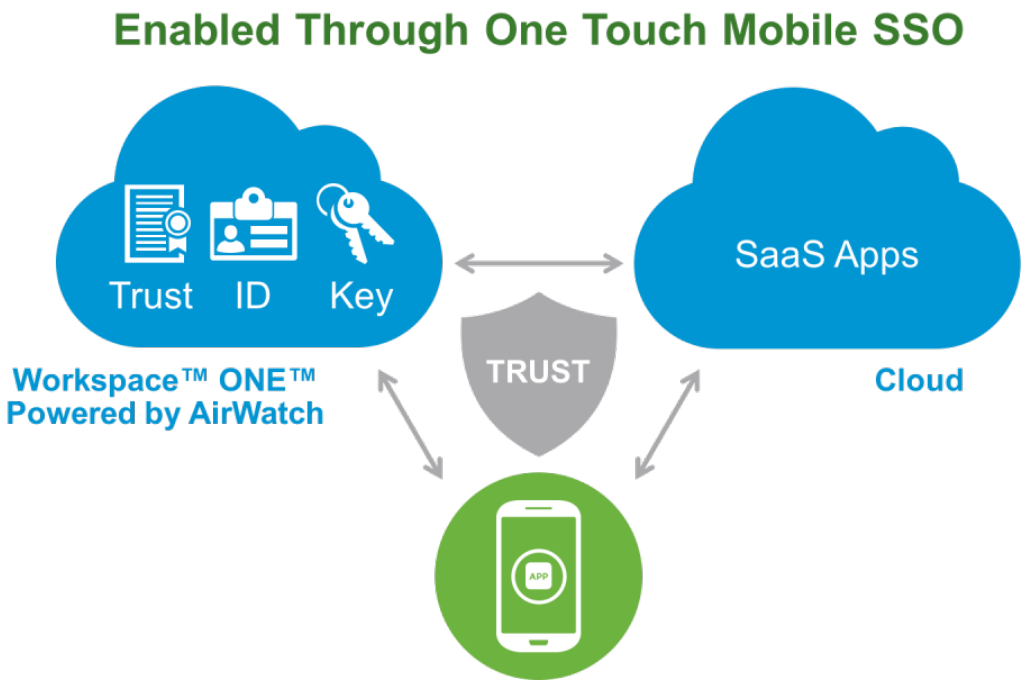
What are the key features of VMware Workspace ONE?

As an IT admin, you want to know about the features right? This section summarizes the key features of Workspace ONE, and outlines a few key examples/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 make this happen, but in so doing you've eliminated the deluge of help-desk calls for end-users to get access to applications and services.

- Provide easy access to all of the apps your end users need to do their job either through a catalog available through a browser or the Workspace ONE native mobile app.
- 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. Through the use of certificates, Workspace ONE provides a secure and easy way that results in a password-less single-sign on experience.



Device management options

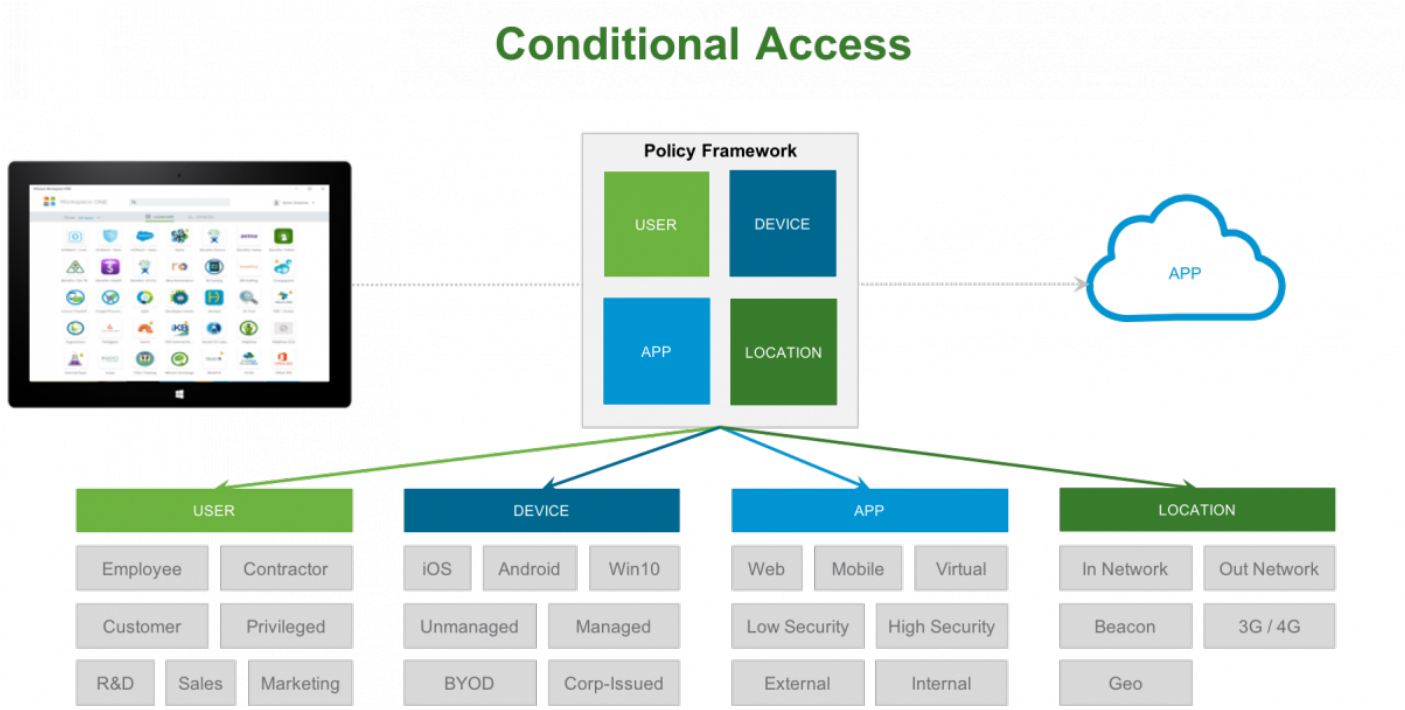
Workspace ONE doesn't dictate which platforms to deploy in your environment. Our goal is to support any device…even devices that have not yet been invented. From desktop OS's to mobile OS's, even wearables, and 3D graphics workstations, we work with it. Beyond that, we also know that some of these devices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

- Desktops OSs, mobile OS, 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, etc…there are so many device management types. Workspace ONE supports them all in a single platform.
- Adaptive management makes the workflow of an end user logging in on a BYO device super simple. Just launch the Workspace ONE app. If the end-user tries to access an app with confidential data, they will be walked through the steps to elevate management on their device.

Network access control

To protect the most sensitive information, Workspace ONE combines identity and device management to enforce access decisions based on a range of conditions from strength of authentication, network, location, and device compliance. We provide a powerful policy engine so that you can mix and match these inputs to make dynamic decisions on the level of access end-users get. This means that if you need to lock down access to sensitive data from remote users on unmanaged devices, you can do that in just a few clicks. But we go one step further. We provide the end-user workflow for endpoints to get into a state that results in compliance, and thereby access.

- Conditional Access policies can be applied on a per-application basis to enforce authentication strength and restrict access by network scope or through any device restriction.
- Advanced data leakage protects against rooted or jailbroken devices, allowlist and denylist apps, open-in app restrictions, cut/copy/paste restrictions, geofencing, network configuration, and a range of advanced restrictions and policies.
- 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, supported by Workspace ONE UEM and Horizon virtualization technology, enables IT professionals to automate application distribution and updates on the fly. Whether you're deploying Windows apps, mobile apps, or even virtualized applications, we automate the application delivery process to enable better security and compliance. This means that whether you need to deploy Windows apps to Windows 10 devices in your organization or up-to-date virtualized apps to mobile devices, Workspace ONE provides a single platform that keeps you covered every step of the way.

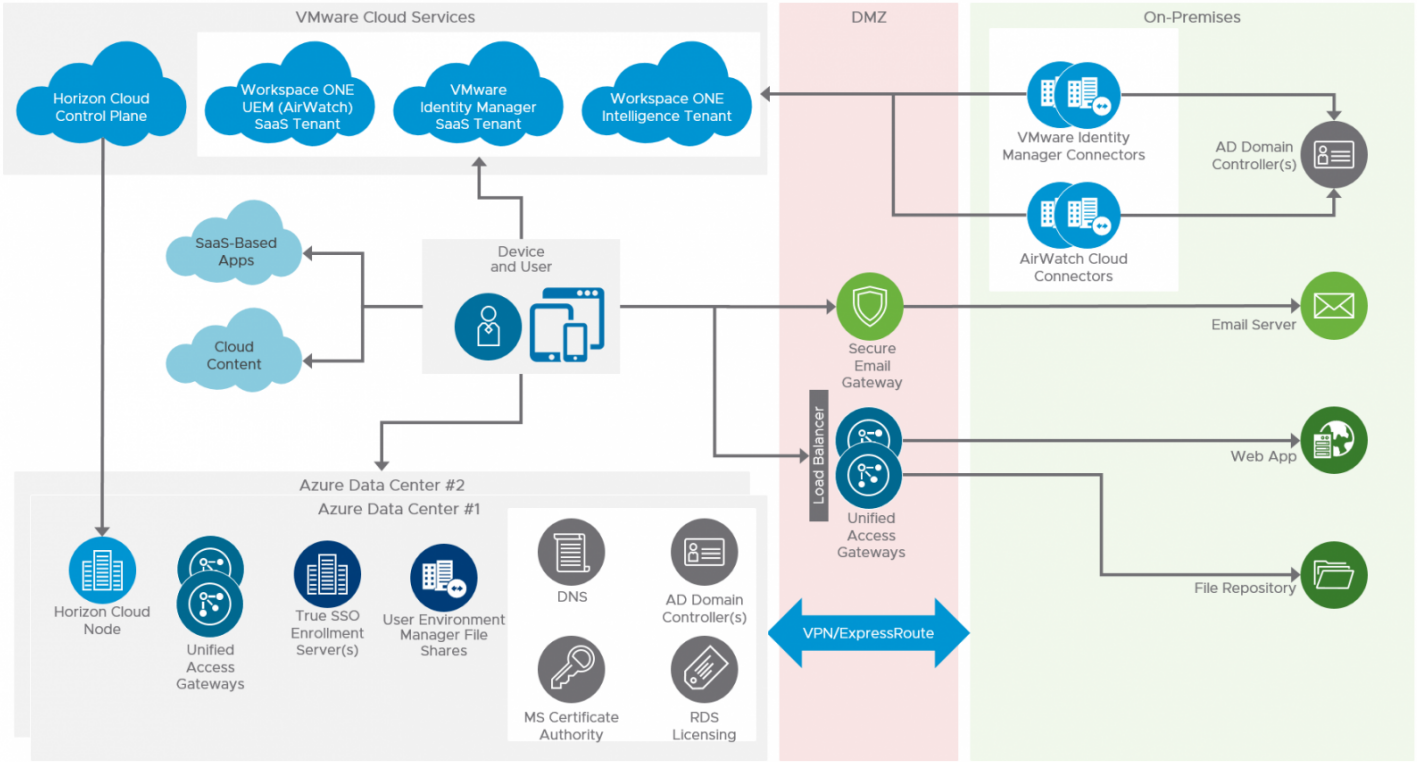
- Simplified management and provisioning of devices enables Workspace ONE to eliminate the need for laptop imaging. With dynamic smart groups, which uses device information and user attributes, you can ensure always have the necessary configuration on their devices, including Wi-Fi and VPN.
- Automatically install, update, and remove software packages. Create an automated workflow for software, applications, files, scripts, and commands to install on laptops, and configure installation during enrollment or on-demand. You can also set the package to install based on a variety of IT-defined conditions.
- Horizon provides secure hosted virtual apps and desktops enabling users to work on highly sensitive and confidential information without compromising corporate data. Users can access their virtual apps and desktops from the Workspace ONE app, enabling them the flexibility to be productive wherever they need to.

Workspace ONE Architecture

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.

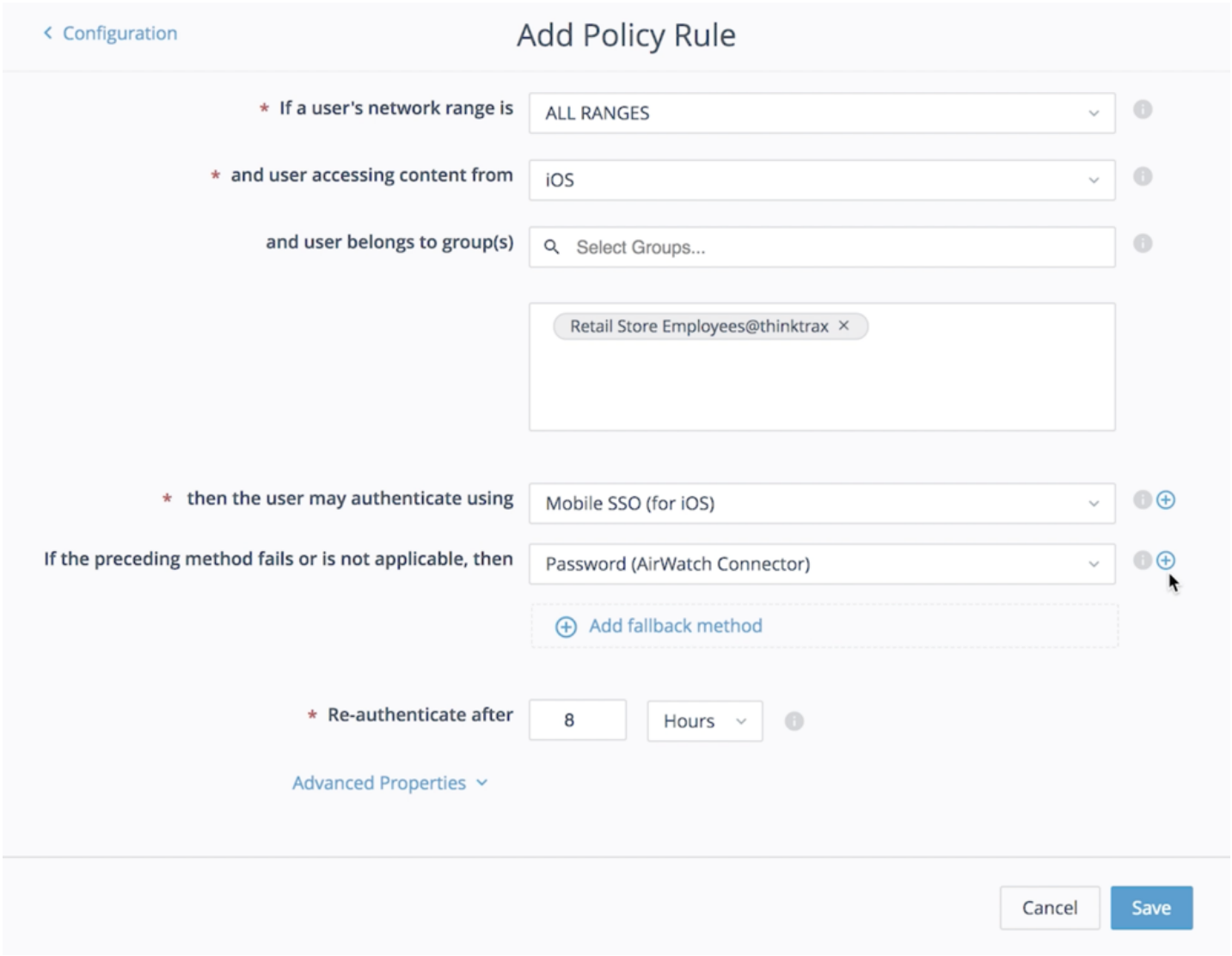
Since the purpose of Workspace ONE is to manage secure application delivery to your end-users, it's critical that you connect Workspace ONE to an existing directory infrastructure. You can configure Workspace ONE to use Active Directory or other LDAP-based directory, for user synchronization, authentication,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

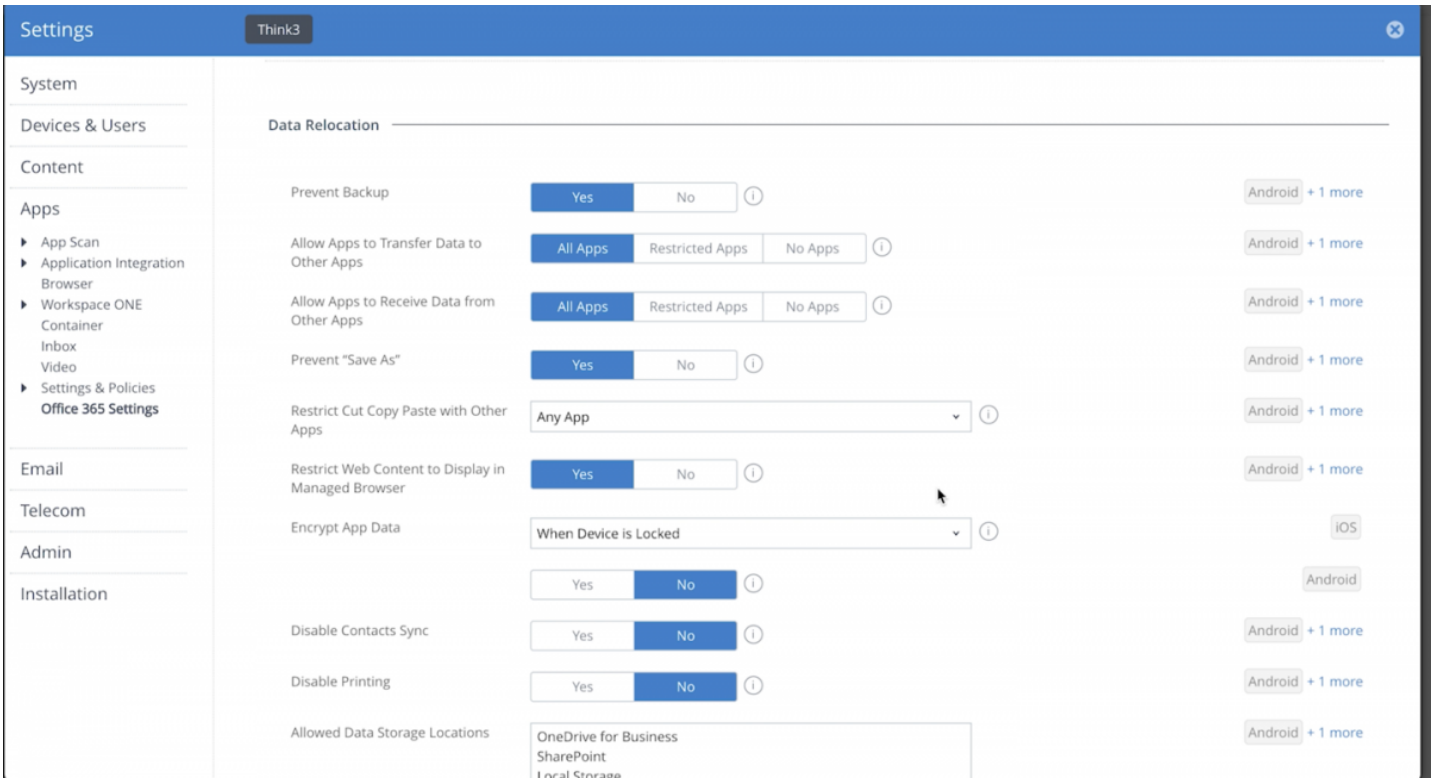


Workspace ONE components

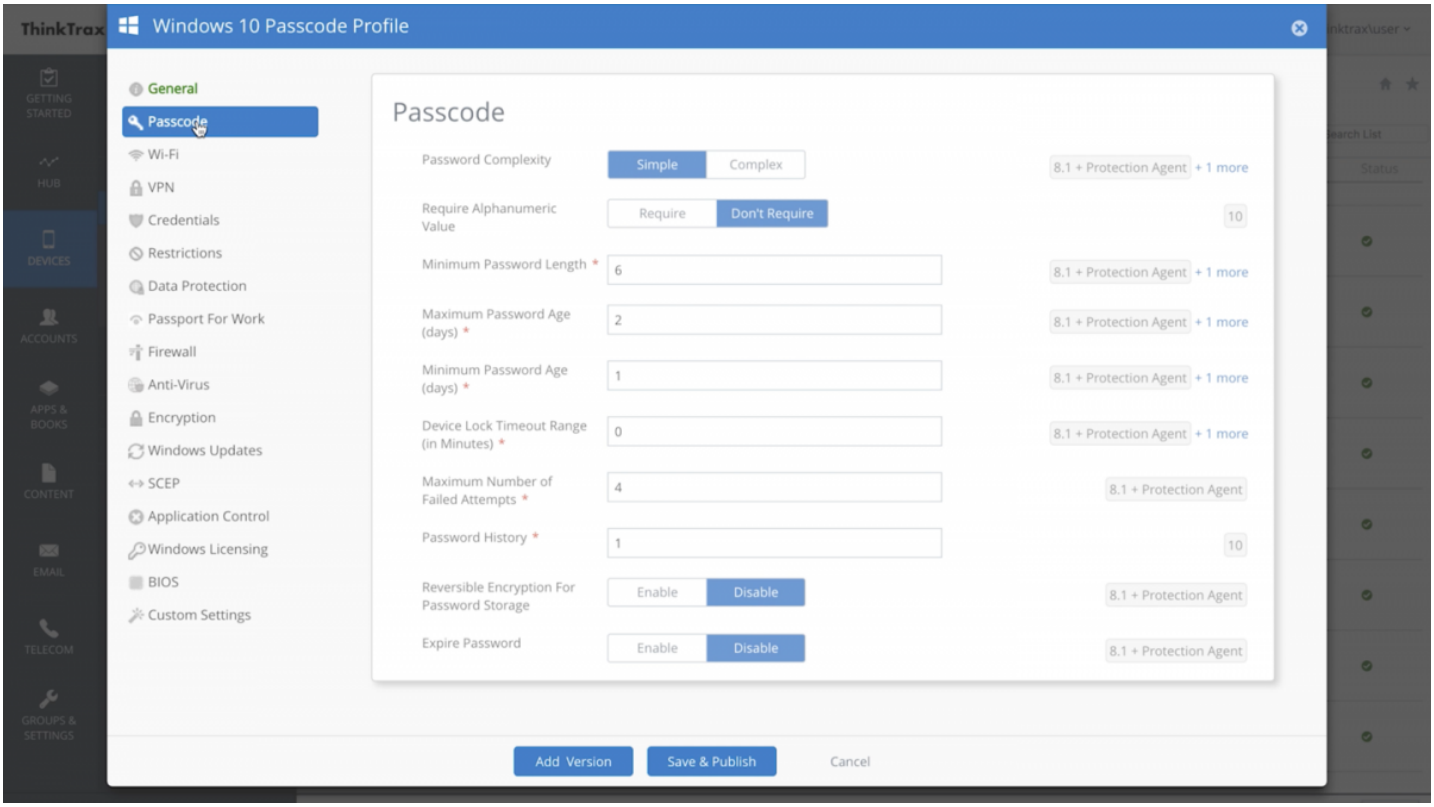
- **VMware Identity Manager** provides single sign-on (SSO) to an application store for software-as-a-service (SaaS)-based Horizon 7, Citrix, VMware ThinApp®, and web applications, as well as for Horizon 7 virtual desktops. It also provides a set of networking and authentication policies to control application access. For example, in the below, 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.



- **VMware Workspace ONE UEM** (formerly known as AirWatch) provides a comprehensive enterprise mobility platform that delivers simplified access to enterprise applications, secures corporate data, and enables mobile productivity. It also works with the public application stores, to handle the provisioning of native mobile applications to mobile devices. The following image shows how 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, etc), but also some features that will really improve the experience for end users (configuring Wi-Fi and VPN for example).



- **AirWatch Cloud Connector (ACC)** – Runs in the internal network, acting as a proxy that securely transmits requests from Workspace ONE UEM to the organization's critical back-end enterprise infrastructure components. Organizations can

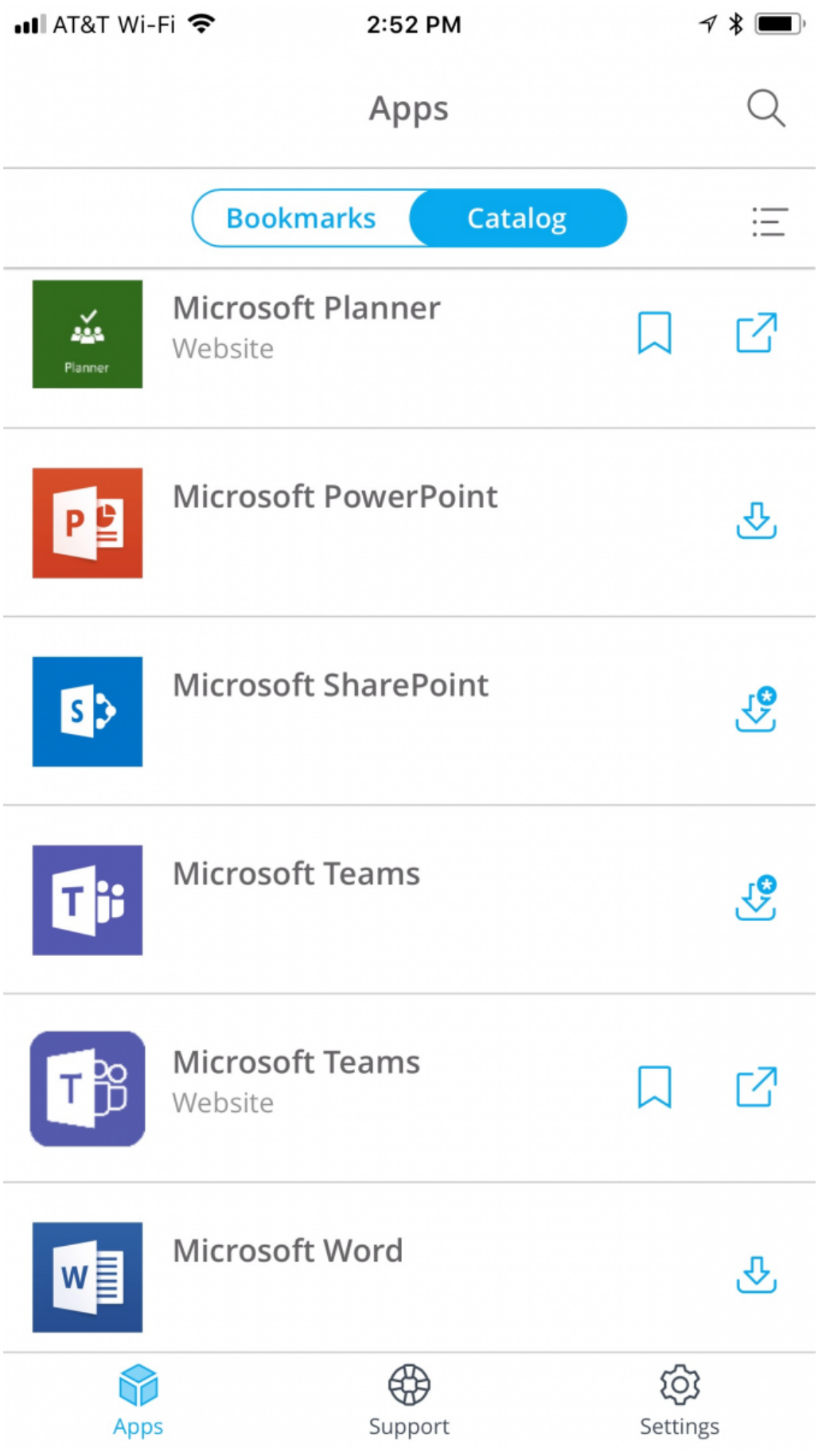
leverage the benefits of Workspace ONE® UEM, running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems.

- **VMware Identity Manager Connector** – Performs directory sync and authentication between an on-premises Active Directory and the VMware Identity Manager service.

Workspace ONE application

The primary end-user component is the Workspace ONE application. Access the application catalog can be done from either the browser or a native mobile application. End-users can install the Workspace ONE native application through the public application store on Android, iOS, and Windows 10. Once installed, end-users will login with their Active Directory credentials and see the applications that IT has enabled access to.

Applications with a star near the download button will require enrolling in management, which means that we will use the device APIs to handle endpoint management and ensure compliance. 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.


AT&T Wi-Fi
2:52 PM
Apps
Bookmarks
Catalog
Microsoft Planner
Website
Planner
Microsoft PowerPoint
Microsoft SharePoint
Microsoft Teams
Microsoft Teams
Website
Microsoft Word
Apps
Support
Settings

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

Want to see Workspace ONE in action?

This demo video walks you through the fundamentals of Workspace ONE.

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.

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