Using Workspace ONE with Office 365

The rapid adoption of Office 365 coupled with the proliferation of powerful yet affordable mobile devices has introduced new challenges in the work environment. With Office 365, end-users have multiple ways to access their email and data: from the browser, native mobile applications, and desktop apps. This has introduced complexity that has never been seen before since each access mechanism has a different authentication flow that must be managed by IT. Due to this complexity and the associate security risks introduced, organizations are looking for solutions that simplify the security and management of access to Office 365.

Many organizations are adopting VMware Workspace™ ONE™ to deliver and manage any app on any device and manage the constant proliferation of mobile devices and BYO programs in the enterprise. By integrating identity management, real-time application delivery, and enterprise mobility management, Workspace ONE enables employees to be productive while completely modernizing traditional IT operations for the Mobile Cloud Era.

Solution Overview

For customers looking to adopt Office 365, there is a need to provide a secure solution for end-users that enables secure access, while providing customized security policies based on the type of access device. With Workspace ONE, Office 365 customers can achieve the following benefits:

- **One-touch single sign-on (SSO) from mobile devices.** Industry leading, seamless, single sign-on (SSO) to public mobile apps using the patent pending Secure App Token System (SATS) establishes trust between the user, device, application, and the enterprise. Multi-factor authentication (MFA) is also available.
- **Block access from unmanaged devices and non-compliant managed devices.** Enforce access decisions based on a range of conditions from strength of authentication, network, location and device compliance. Advanced data leakage protection also restricts access from rooted or jailbroken devices.
- **Office 365 Application Access Control.** Automatically deploy Office 365 applications if an authenticated user has logged into a managed device. In addition, powerful policies enable IT to restrict specific Office 365 services based on users or groups.
- **Secure Content Collaboration.** Protect your sensitive content in OneDrive in a corporate container and provides users with a central application, AirWatch Content Locker, to securely access, store, update and distribute the latest documents from their mobile devices.
- **Consumer Simple, Enterprise Grade Email Client.** With VMware Boxer (part of Workspace ONE) end-users get an intuitive experience with a host of advanced mail, calendar and contacts features inside of one containerized app and IT admins get the ability to configure and manage security policies at a granular level.

This document provides a high-level overview of the architecture and end-user experience to achieve these benefits.

Authentication Flow

When Office 365 receives a request for authentication, it will send that request to Identity Manager (part of Workspace ONE). Identity Manager will then enforce different single sign-on (SSO) authentication policies based on the type of device and the compliance state of the device. Once authentication is successful, the SAML assertion will be sent back to Office 365.

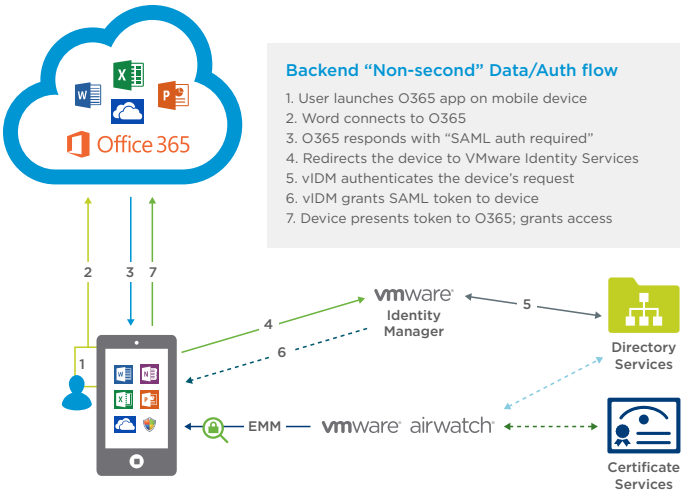

Figure 1: Authentication flow for an end-user accessing Office 365 from a Workspace ONE managed mobile device

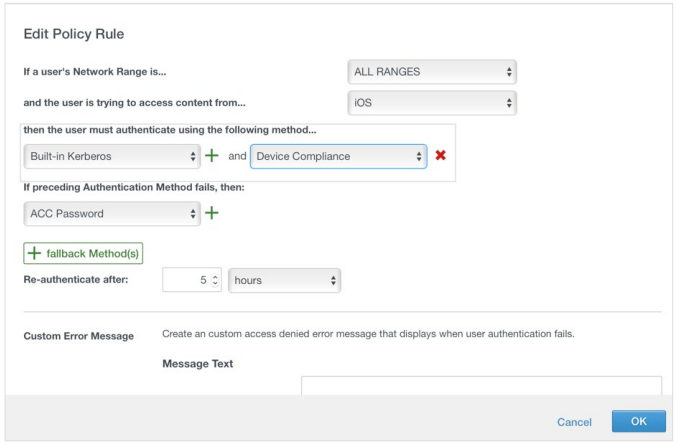

Figure 2: Access to Office 365 applications can be blocked when a device goes out of compliance. When the device is brought back into compliance, then the user can access Office 365 applications.

End-User Experience

Workspace ONE uses a secure application token to silently authenticate the user behind the scenes. A secure cryptographic app token in the form of certificate is provisioned onto the device that allows Workspace ONE with Identity Manager to verify who the user is and if the device is trusted or not. In the example below, an end-user launching OneDrive from their mobile device will be redirected so that Workspace ONE can authenticate the user. This happens seamlessly for the end-user without any requests for additional passwords.

Figure 3: Seamless access to OneDrive with Workspace ONE

Summary

For customers looking to adopt Office 365, Workspace ONE enables secure access from mobile devices, while providing customized security policies based on the type of access device. This ensures that end-users get consumer simplicity, with an experience that is seamless and easy to use while IT can ensure that only compliant users and devices access corporate resources such as Office 365.

Together, Office 365 and Workspace ONE, work seamlessly to provide a secure experience for access to applications and data, so that end-users can be productive from any device, anywhere.

To learn more about Workspace ONE, visit our website at http://www.vmware.com/products/workspace-one.

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