AirWatch Support for Office 365
One of the most common questions being asked by many customers recently is “How does AirWatch support Office 365?” Customers often ask if VMware AirWatch® can control access to Microsoft Office 365 not only on their corporate systems, but most importantly on their mobile devices.

Fortunately, AirWatch provides comprehensive support to help organizations leverage Office 365 on their mobile devices:

• AirWatch makes it easy to deploy the Office apps and email to the users that are licensed for them, and sets the users up so they sign in automatically to the apps using the same identity as their corporate account.

• Integration with VMware® Identity Manager provides an industry-first adaptive access control framework to ensure that all work applications, including Office 365, can only be installed and run on managed and compliant devices.

• Containerization that relies on the native OS Mobile Application Management (MAM) controls ensures encryption of data at rest, prevents corporate data leakage, and supports enterprise (selective) wipe of devices.

The Office 365 Challenge

Migrating to Office 365 for an organization presents a host of new challenges:

• Given that Office 365 is accessible from the Internet, traditional access control mechanisms for email and apps, which are based on network and perimeter security models, fail to work.

• Unlike their desktop equivalents, mobile Office apps present new, complex data protection challenges for BYOD users - including containerization and remote wipe.

What organizations need is a way to restrict O365 access to only managed and compliant devices without any dependency on the network or domain membership. Additionally, they need to ensure that any data stored on a device is encrypted and can be remotely wiped if lost or stolen. While this may seem trivial at first, it gets increasingly complex considering the many platforms and the complexity in enabling the ability for the solution to co-exist with both enterprise mobility management (EMM) and domain managed devices. Complexity is also added when integrating EMM and domain managed devices with existing on-premise infrastructure.

While this white paper specifically discusses how AirWatch solves these problems for O365, the same architecture secures all company applications both cloud and on-premise.
AirWatch O365 Integration

AirWatch enables Office 365 ease of use by providing a common identity for authentication, conditional access control to the apps, and protection for data on the device. Not only is this great news for IT and security, but AirWatch also enables easy scaling of the Office 365 apps across the organization by making the entire provisioning process simple and automated for the end users.

Self-Service Secure SSO Access to O365

Provision Office 365 Apps
To begin with, a unified app catalog and EMM capabilities enables IT to securely distribute, or end users to independently download native Office 365 applications and set up email on their mobile devices. AirWatch makes the process of provisioning access to different Office 365 applications easy and automated by syncing with existing on-premises Active Directory (or LDAP) user groups. This ensures only authorized users with purchased licenses are able to access Office 365 services, and automatically revokes access to unauthorized users without requiring any IT involvement or calls to the help desk.

Today, the activation and de-provisioning process are two decoupled processes of (1) revoking access from the identity management system and (2) remotely wiping data and applications from the endpoint device. AirWatch brings these two workflows together to automate and streamline the process.

Simplify Authentication for Office 365 Apps
Once the applications are deployed, AirWatch provides end users with an effortless authentication experience. Integration of AirWatch with VMware Identity Manager enables organizations to easily federate their existing on-premises corporate identity (e.g. LDAP or Active Directory) and automatically single sign-on (SSO) into Office 365 and other web, internal, and public store apps. This enables users to install the app from the app store and automatically authenticate without being prompted for a separate login.

One of the common challenges with using traditional identity solutions is that they fail to work for native mobile applications. The identity module in AirWatch solves this problem by integrating the single sign-on frameworks built around EMM to automatically authenticate all native and web applications seamlessly. This enables the same SSO experience for native mobile apps that a user expects from web or SaaS apps.

Certificate-based Authentication
AirWatch can also leverage digital certificates to automatically sign the user into Office 365; providing password-less authentication. Not only is the user experience superior but security is increased by using certificates to authenticate rather than Active Directory passwords. Since AirWatch installs the certificate in a single secure location, all applications on the device can leverage this identity for authentication.

Certificate-based authentication increases security from two perspectives. First, since AirWatch stores the user’s identity in a single location in the OS, company credentials are not stored or accessible by the applications on the device. This means IT does not have to worry about how each application might be storing a user’s credentials and minimizes the risk of a single application getting exploited. Secondly, since a digital certificate is used rather than a username and password, security is greatly increased. If a device is stolen, the certificate can easily be revoked and access to that specific mobile device can be fully denied without forcing the user to change their password across all company systems and services.
**Integration with Other Third Party Identity Access Management Tools**

While AirWatch provides seamless integration with VMware Identity Manager, it also integrates with existing identity solutions that organizations might already be using. This ensures that current configurations and federated authentication policies can continue to exist while still providing a better SSO and conditional access framework for mobile and managed devices.

The diagram below outlines how the same configuration can co-exist with an organization’s existing third party identity tool (Ping, Okta, ADFS, Azure AD, etc.).

**Conditional Access to Authorized Users and Devices**

In general, only authorized users on authorized devices should be granted access to company applications. For Office 365 this means services such as Exchange Online, OneDrive for Business, Skype for Business, etc. should be restricted to only compliant and managed devices. AirWatch integrates with both Office 365 APIs and VMware Identity Manager to provide conditional access to all Office 365 services.
Exchange Online
AirWatch integrates directly with Exchange Online to restrict email. This is done by first setting up a whitelist policy in Exchange to deny email access as a default behavior for all unknown devices. AirWatch then integrates with Exchange Online to automatically add managed and compliant devices to a “whitelist” so they are authorized to sync email. If a user activates a new device or an existing device goes out of compliance, AirWatch automatically blocks email access on the device by syncing the changes with Exchange Online. AirWatch integration works directly with Office 365 so devices can connect from any network without forcing email traffic through a VPN or on-premises gateway.

Office 365 Apps
In addition to email, AirWatch integration provides the same conditional access to all other Office 365 applications. When a user attempts to access Office 365 and authenticate, Office 365 redirects the authentication to VMware Identity Manager as part of the federated configuration. The authentication not only validates the user identity but also validates that the device is managed and compliant by AirWatch. If a user tries to connect to Office 365 from an unmanaged mobile device, access is denied.

One of the differentiating advantages with this architecture is the flexibility to require different claims rules for authentication based on the device platform and app requesting access. This enables organizations to have different policies for mobile devices than from existing domain joined company PCs. For example:

- Apple iOS and Android native applications can require authentication using certificates
- Windows native applications can require domain membership and authentication
- Web-browser based sessions can have limited access or be required to be on the company VPN or network to access Office 365
Containerize and Protect Data

In addition to having a common identity, SSO experience and conditional access to only managed devices, companies must also ensure Office 365 data is protected on the device itself. This includes ensuring:

- The device is encrypted
- Policies are set to prevent data leakage
- Office 365 data can be remotely wiped from the device if lost or stolen

Containerization and DLP Controls

By deploying Office 365 apps through AirWatch Catalog, AirWatch enforces containerization of these applications to prevent data loss using the native platform controls. Each OS supports different containerization controls as outlined below:

**Apple iOS:**
AirWatch integrates with Apple’s managed app containerization technology to prevent data loss from work and personal applications. This includes preventing Exchange Online emails from being moved from the work account to personal account, and managing the “open-in” controls to prevent email attachments from being saved into personal applications. The same policies work across all Office 365 applications.

**Android (Android for Work):**
Android for Work is a new security container for select Android devices, which enables the Office 365 applications and email to be deployed inside an app container via AirWatch. This ensures Office 365 data is encrypted, managed and can be remotely wiped and data leakage between work and personal apps is avoided. Furthermore, organizations can enforce advanced data loss prevention controls such as screen capture and copy/paste restrictions.

**Windows:**
AirWatch supports flexible deployment options using either AirWatch® Inbox (Windows 8.1) or native mail client (Windows Phone 8.1) to ensure email setup on the device is restricted to managed devices and can be remotely wiped from the device.

**Windows 10** will add an additional layer of Enterprise Data Protection (EDP) for work apps to prevent sharing Office 365 data to personal apps and preventing commands like copy/paste actions between work and personal applications. AirWatch is excited to partner with Microsoft in supporting EDP capabilities for organizations participating in Microsoft TAP program and certain Windows Insiders builds. AirWatch EDP features for Windows Insiders build enable organizations to designate trusted desktop or modern apps, including Office 365 apps, with permission to open or decrypt work data. Flexible enforcement levels in AirWatch can either enable or disallow certain user groups from data moving and sharing capabilities, such as copy/paste, drag and drop, and others.
Enterprise Wipe

78% participants of a mobile security survey identified lost or stolen devices containing company information as their top mobile security concern. In the same study, 45% participants reported that their employees actually lost a mobile device in the past one year with corporate data on it.¹ Enterprise Wipe capability in AirWatch enables organizations to selectively wipe all corporate data and apps, including removing Office 365 services, from a lost or stolen device. All of the enterprise data contained on the device is removed, including mobile management profiles, policies and internal applications. The enterprise wipe can be executed by the IT admins, or more reactively by the employees themselves using the AirWatch Self-Service Portal (SSP).

Additional Office 365 Security Settings

Office 365 has a few application settings that prevent copy and paste, require a PIN to launch the app and disable “Save As” to other non-work related storage locations (e.g. Dropbox) from within the Office 365 applications themselves. Much like a SalesForce¹ mobile app or a SAP Concur app has settings for application behavior and features to turn On or Off, the copy and paste, PIN, and Save As settings are application specific controls Microsoft has built into their software. Today, these controls and settings are not extensible to third party management systems or tools to configure; therefore, they must be configured from the application itself and requires the use of Microsoft InTune MAM as the management tool to deliver these app settings.

Many other ISVs (e.g. Oracle, Cisco, Salesforce, and others) however, take standard app configuration approaches such as using iOS managed app profiles. We are hopeful Microsoft will extend these Office 365 app settings to be configured differently in the future (directly through AirWatch) so organizations have a consistent framework to manage configurations and settings for all enterprise applications. Following recent product updates by Microsoft, organizations can now use Intune MAM alongside existing EMM solutions. This co-existence enables organizations to leverage above Office 365 DLP settings using Intune; and extend the capabilities further with AirWatch, which ensures support for multiple platforms, app types, and device ownership use cases (BYOD, CYOD, corporate-owned, corporate-shared).

Summary

Today, 60% of organizations are going beyond basic productivity (email and Office apps) and are deploying new apps or reengineering core business processes to support their mobile workforce.² Organizations that have made such investments in Line of Business (LOB) apps need to ensure that their EMM solution integrates with all of the enterprise app investments and supports multiple device ownership scenarios. VMware AirWatch® Enterprise Mobility Management™ provides a holistic and extensible solution that is vendor-agnostic and uses a standard application configuration approach.³ This ensures organizations have a unified management solution, which not only fully integrates with the Office 365 suite of applications, but also all other ISV applications and services (cloud and on-premises), app development platforms, and proprietary applications that they want to provision and secure.


Additional Resources

For additional information, visit www.air-watch.com/solutions/windows.

To get started with a free trial of AirWatch, visit www.air-watch.com/free-trial.

AirWatch Global Headquarters
1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch
AirWatch is the leader in enterprise mobility management, with a platform including industry-leading mobile device, email, application, content, and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at www.air-watch.com.