



AirWatch Support for



Office 365

AirWatch Support for Office 365

One of the most common questions being asked by many customers recently is “How does AirWatch support Office 365?” Many ask if AirWatch can control access to Office 365 (O365) not only on their corporate desktop systems, but most importantly on their mobile devices.

Fortunately, AirWatch® by VMware® provides tremendous support to help organizations leverage O365 on their mobile devices and our recent integration with VMware® Identity Manager provides an industry-first adaptive access control framework to ensure that all work applications, including O365, can only be accessed on managed and compliant devices.

The Office 365 Challenge

Migrating to O365 for an organization presents a host of new challenges. First, given that O365 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. Secondly, unlike their desktop equivalents, mobile office apps present new, complex 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 users to easily use O365 by providing a common identity for authentication, providing conditional access control to ensure only managed devices gain access and containerize the data on the device to ensure it's secure and can be remotely wiped. Not only is this great news for IT and security, but AirWatch also enables self-service provisioning of O365 access by end users to make the entire process simple and automated; allowing easy scaling of O365 across the entire organization.

Self-Service and Secure SSO Access

To make an effortless user experience, integration of AirWatch with VMware Identity Manager allows organizations to easily federate their existing on-premise corporate identity (e.g. LDAP or Active Directory) and automatically single-sign-on (SSO) into O365 apps. This allows users to navigate to a single webpage portal, login with their company credentials and easily get access to email, Lync, and all other Office apps without having to re-enter credentials for every single app.

In addition to web based apps, AirWatch® Catalog and EMM capabilities allow users to securely download native O365 applications and set up email on their mobile devices.

One of the most unique advantages AirWatch and VMware Identity Manager provide is to configure the same SSO experience a user expects from web applications using the native mobile apps.

AirWatch can also leverage digital certificates to automatically sign the user into O365; providing passwordless authentication. Not only is the user experience superior but security is increased by using certificates to authenticate rather than AD passwords. Since AirWatch installs the certificate in a single secure location, all applications on the device can leverage this identity for authentication.

This 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.

AirWatch also makes the process of provisioning access to different O365 applications easy and automated by syncing with existing Active Directory (LDAP) user groups. This ensures only authorized users with purchased licenses are able to access O365 services and automatically revokes access to unauthorized users without requiring any IT involvement or calls to the help desk. Today, the activation and deprovisioning process are two decoupled processes of revoking access from the identity management system and remotely wiping data and applications from the endpoint device. AirWatch brings these two workflows together to automate and streamline the process.

Conditional Access to Authorized Users and Devices

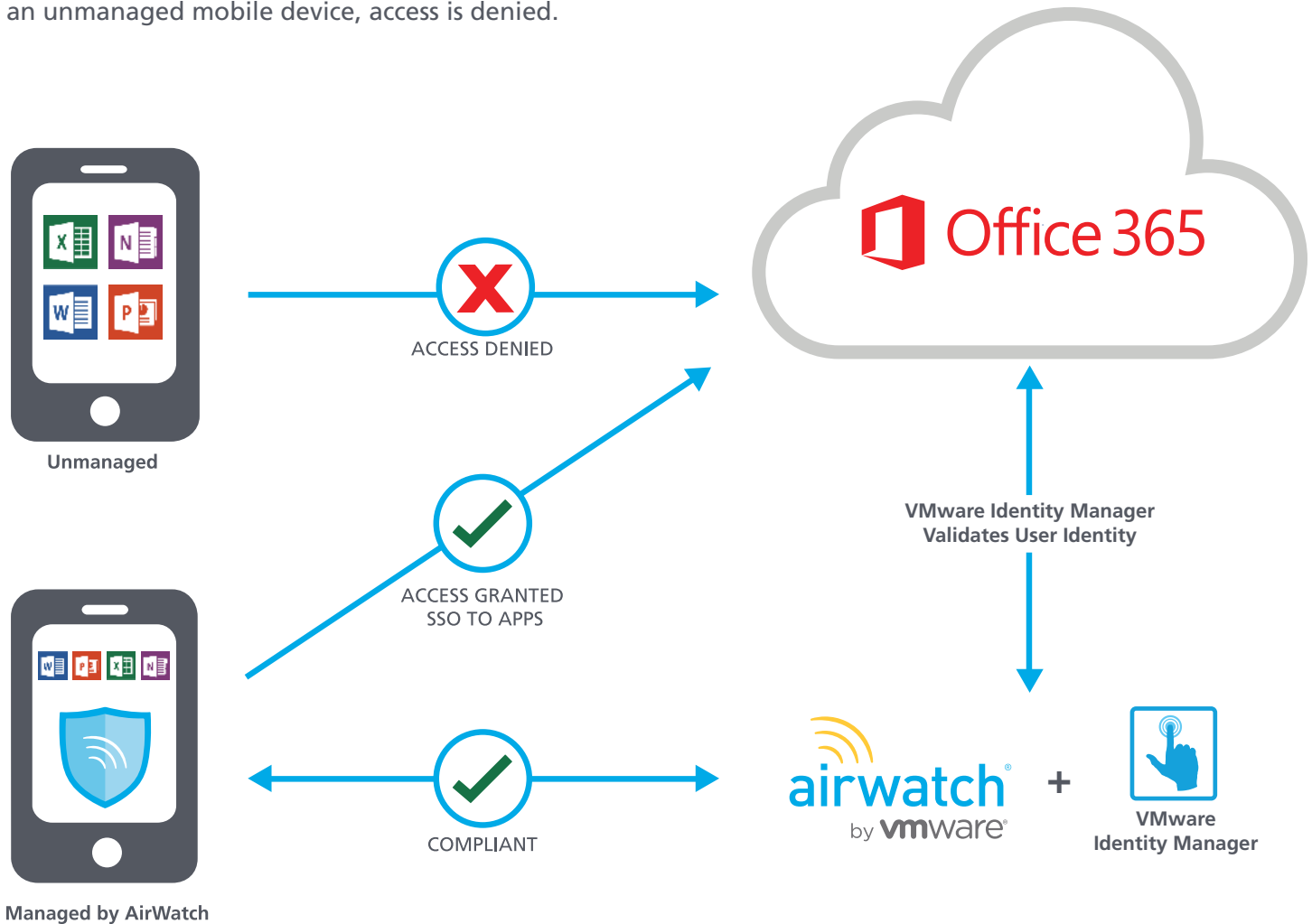
In general, only authorized users on authorized devices should be granted access to company applications. For O365 this means services such as Exchange Online, OneDrive, Lync, etc. should be restricted to only compliant and managed devices. AirWatch integrates with both O365 APIs and VMware Identity Manager to provide conditional access to all O365 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 syncs the changes with Exchange Online. AirWatch integration works directly with O365 so devices can connect from any network without forcing email traffic through a VPN or on-premise gateway.

O365 Apps

In addition to email, AirWatch integration provides the same conditional access to all other O365 applications. When a user attempts to access O365 and authenticate, O365 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 O365 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 allows organizations to have different policies for mobile devices than from existing domain joined company computers. For example:

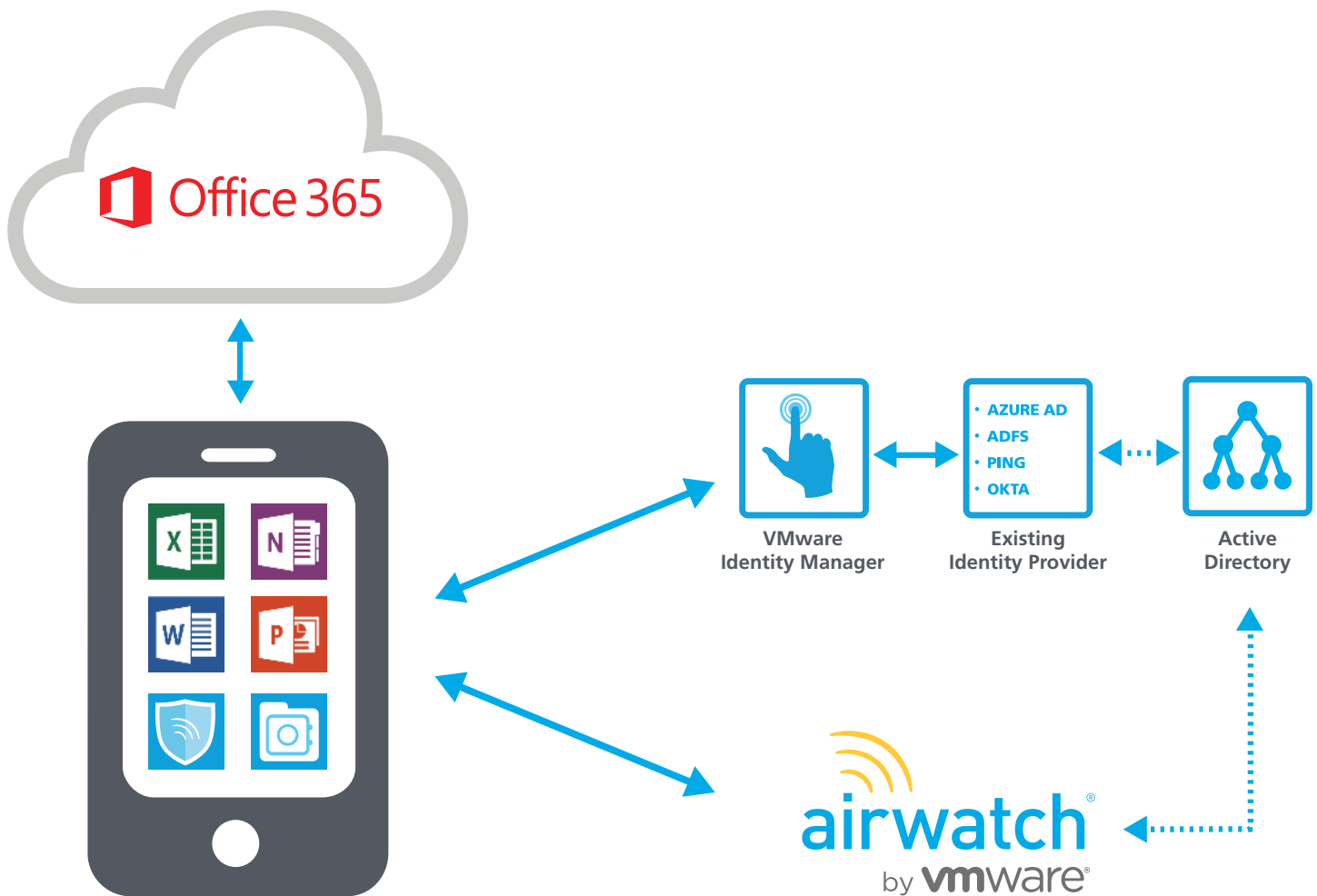
- Apple iOS native applications can require authentication using certificates
- Android native applications can require authentication using certificates
- Windows native applications can require domain membership and authentication
- Web-browser based sessions can have limited access or be required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

to access O365

Integration with Other Third Party Identity Access Management Tools

While AirWatch provides seamless integration with VMware Identity Manager and is included in the [AirWatch Blue and Yellow Management Suites](#), AirWatch can also integrate 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.).



Supported O365 Applications

Microsoft has made great efforts this year to update their O365 native applications across all platforms and is continuing to provide updates on a monthly basis. Some apps and platforms are still waiting for Microsoft to support a federated authentication flow inside the application before AirWatch can fully provide conditional access and a seamless SSO experience.

Containerize and Protect Data

In addition to having a common identity, SSO experience and conditional access to only managed devices, companies must also ensure O365 data is protected on the device itself. This includes ensuring the device is encrypted, policies are set to prevent data leakage and ensuring that O365 data can be remotely wiped from the device if lost or stolen.

By deploying O365 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 and managing the "open-in" controls to prevent email attachments from being saved into personal applications. The same policies work across all O365 applications.
- **Android (Android for Work):** Android for Work is a new security container for select Android devices which allows the O365 applications and email to be deployed inside an app container via AirWatch. This ensures O365 data is encrypted, managed and can be remotely wiped and data leakage between work and personal apps is avoided. Furthermore, DLP controls such as screen capture and copy/paste restrictions are enforced.
- **Windows:** AirWatch allows 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](#) adds an additional layer of Enterprise Data Protection (EDP) for modern apps to prevent sharing O365 data to personal apps and preventing commands like copy/paste actions between work and personal applications.

Additional O365 Security Settings

O365 has a few application configurations 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 O365 applications themselves. Much like a social networking application might have settings for application behavior and features to turn on or off, these 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.

Configuring these settings requires the use of InTune MDM as the management tool to deliver these app settings. Many other ISVs (Salesforce, Box, etc.) take standard configuration approaches using iOS managed app configurations and it is unclear if Microsoft will extend these same settings to be configured differently in the future. AirWatch would prefer a more standard approach to enable these settings within their applications so organizations have a consistent framework to manage configurations and settings for all enterprise applications.

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 by VMware

AirWatch by VMware 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.