VMware Identity Manager

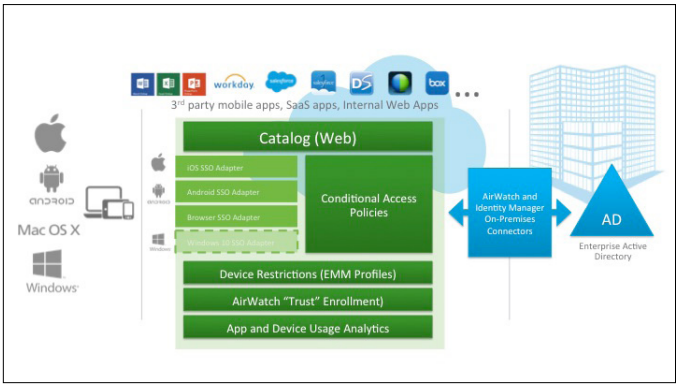
Identity Management for the Mobile Cloud Era

AT A GLANCE

VMware Identity Manager™ is identity management for the mobile/cloud era that delivers on consumer-grade expectations like one-touch access to apps, optimized with AirWatch Conditional Access and backed by a self-service app catalog with enterprise-class management and security expected from the leader of hybrid cloud infrastructure.

KEY BENEFITS

- Empower employees to be both happy and productive; removing the traditional barriers to mobility like complex passwords, configuration steps, traditional VPNs and tokens by uniquely optimizing authentication for each device type rather than the lowest common denominator.
- Free the business to roll out new SaaS and mobile apps and services immediately to forever change business processes and customer engagement while maintaining a single point of user entitlement and license monitoring.
- Simplify IT by leveraging existing directory infrastructure and extend to SaaS and mobile apps with automated provisioning, utilization reporting and conditional access policies.



What Is VMware Identity Manager?

VMware Identity Manager is identity management for the mobile cloud era that delivers on consumer-simple expectations like one-touch access to nearly any app, from any device, optimized with AirWatch Conditional Access. Empower employees to get productive quickly with a self-service app store while giving IT a central place to manage user provisioning and access policy with enterprise-class directory integration, identity federation and user analytics expected from the leader of hybrid cloud infrastructure.

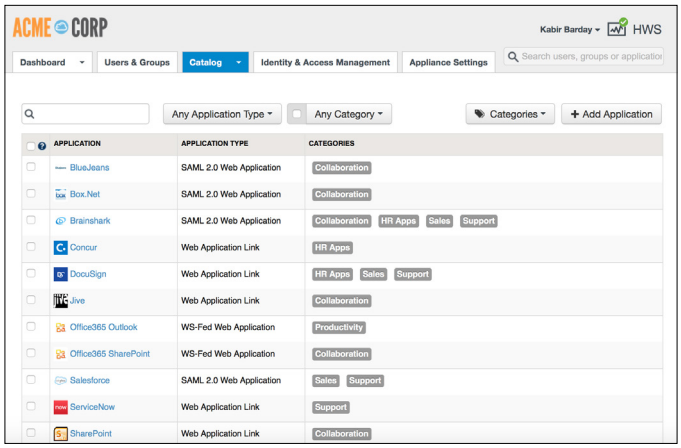
How Is Identity Manager Used?

Mobile and SaaS App Delivery

Most enterprises today have at least one or two SaaS apps in use. Typically, a line of business owner who owns the function of the app manages application provisioning and user management manually. At best, they may coordinate with IT for help desk and ticket management for new user onboarding, separation, or password resets. While this might be OK for one or two SaaS apps, many enterprises are now deploying their third, fourth or fifth app, with their corresponding mobile apps making these manual processes too complex. This complexity risks compliance and security as no one in IT can guarantee what employees have access to what apps, or what data might be saved on unmanaged, unencrypted devices. Using VMware Identity Manager with AirWatch® Enterprise Mobility Management™, IT has one infrastructure for managing users across both app types and device types.

Accelerating Office 365 Deployments

Many enterprises are planning Office 365 deployments if only to help simplify their Exchange environments by moving to Exchange Online. Then organizations may want to extend Office 365 apps to unmanaged devices and then native mobile iOS, Android, and Windows 10 Office apps. While they may already be licensed to take advantage of all Office 365 has to offer, Office 365 uses a completely separate Azure AD directory and synchronization proves too challenging with existing complex Active Directory infrastructure. VMware Identity Manager federates the existing on-premises Active Directory to maintain one source of truth and accelerate deployment.



Key Features

Simplify Business Mobility with One Touch from Any Device

In the mobile cloud era, IT must assume that users are mobile and that their devices are likely unmanaged. For users to be productive, they must access their apps and data the same way, no matter where they are and it needs to "just work" without the complexities of multiple user accounts, passwords, and other complex authentication methods.

Enterprise Single Sign-On	Single-Sign-On eliminates the need for users to remember multiple usernames and/or passwords to access the disparate apps and systems they use for work. Beyond saving the hassle and expense of service desk calls, federating user identity also ensures that access to apps can be turned off at a single point protecting against data leakage in the event of employee separation. VMware Identity Manager includes an identity provider (IDP) or token generator but it can also integrate with existing identity providers that may already be in place to aggregate SSO apps into one convenient catalog and launcher across any device type.
Industry-leading support for Web, virtual desktops, published applications, Windows packaged apps, and native mobile apps, all from one place	VMware Identity Manager uniquely supports a wide range of web, virtual and natively installed applications all from one place. Windows applications may be accessed through VMware ThinApp® packaged application delivery to managed or unmanaged, non-domain joined laptops. Windows apps may also be accessed through Citrix XenApp or from Horizon 6 app delivery or complete VDI desktop delivery. Web applications are supported through SAML for applications such as Google Apps, Salesforce, Box, ServiceNow, and WS-Fed for Office365.
Preintegration with many enterprise apps	VMware works with a range of enterprise SaaS vendors leveraging the SAML standard to provide pre-defined integrations including automated user provisioning.

Empower Employees with a Self-Service App Store

Today, apps and information are everywhere, both inside and outside the walls of your datacenter. IT is under more pressure than ever to secure and manage this new changing landscape but the old methods of deploying apps in a desktop image and securing remote access with a general-purpose VPN doesn't work in a mobile/cloud world. VMware Identity Manager manages the complete user lifecycle across the hybrid cloud complete with a custom brandable launcher and app store application provisioning, and user analytics to monitor and manage resources.

Self-service app catalog	The VMware Identity Manager app catalog is a one-stop shop for enterprise applications. Self-service means that instead of entering tickets, employees can simply search and select applications that they want to subscribe to and kick-off automated or manual provisioning as required.
Responsive HTML5 app launcher	Support *any* device through a responsive and skinable web app that includes simple sorting by category and favorites.
User analytics	Most enterprises may know how many apps are in use, but they have little idea just who is using them or how often. With VMware Identity Manager, all application access flows through the service enabling detailed reporting on usage. Easy to use analytics help you understand usage trends, capacity planning and licensing management powered with rich and detailed information.
Custom-brandable Web portal	Make it your own. In just a few minutes, the VMware Identity Manager customization tool allows you to transform the self-service app store and launcher with your colors, logos, backgrounds, textures and design elements.
Application provisioning	Once a new application is placed in the app catalog, administrators may auto-provision to users by group, or enable self-subscription. VMware Identity Manager permits subscription events to kickoff approval workflows through existing partners like Remedy.

Optimize User Experience and Security—with AirWatch Conditional Access

VMware Identity Manager was designed for the mobile cloud world with industry-first mobile device optimizations for AirWatch enrolled devices. By following the AirWatch device registration process, Conditional Access is established between the user, their device, and the hybrid cloud adding additional security, but more importantly a seamless consumer-grade user experience.

Conditional access	VMware Identity Manager can apply conditional access policies by user security group, network, and authentication strength.
Managed or unmanaged device: conditional access	Not all apps should be treated the same as they can carry different risks of data loss. VMware Identity Manager can distinguish between managed and unmanaged devices to allow broad access to low risk apps and then enforce device management with encryption and wipe controls for apps that contain sensitive data.
Native integrated app launcher	Adding AirWatch EMM integrates subscribed applications into the AirWatch catalog where they can be "installed" directly onto the native springboard as just another application icon, ready for use.
Device analytics	Beyond app usage analytics, device analytics supplied through AirWatch enrolled devices permit IT to understand the intersection of apps and devices to make intelligent decisions about capacity planning and new service development.

Grow with Trusted VMware Enterprise-Grade Hybrid Cloud Infrastructure

VMware Identity Manager leverages the same core identity management solution that may be seen powering VMware vCloud Air and the vCloud Suite in the world's most advanced datacenters and enterprise-class infrastructure clouds. This experience enables us to tackle complex enterprise directory structures with modular, standards- based architecture permitting nearly any type of authentication. VMware Identity Manager also contains a powerful conditional policy engine and can seamlessly integrate with industry leading infrastructure such as F5.

Directory integration and federation	Supports multiple Active Directory domains, multiple forests and different trust configurations offering extreme flexibility for integrating with existing environments.
Hybrid deployment model	VMware Identity Manager is built from a single multi-tenant code base whether deployed on premises, or in the cloud. Cloud-based and on-premises instances of VMware Identity Manager may federate for added flexibility.
Universal authentication broker	Beyond the trust established between the user, a device, and the datacenter, additional layers of authentication may be brokered through VMware Identity Manager such as biometrics APIs in mobile devices, third-party biometrics or tap-and-go systems from partners like Imprivata, and a range of adaptive authentication from vendors such as RSA.

How to Trial and Buy

VMware Identity Manager Advanced Edition is available through standalone licensing or as part of AirWatch Blue and Yellow Management Suites and VMware Workspace Suite™. VMware Identity Standard Edition is offered as a part of VMware Horizon® 6 Advanced and Enterprise.

VMware Identity Manager is available as perpetual licensed software for on-premises deployments through an easy to deploy virtual appliance, or as a highly available shared SaaS service that runs on VMware vCloud® Air™ in North America, EU, and Asia Pacific site locations.

See the following site for the latest locations and terms of service: http://www.vmware.com/download/eula/identity-manager-terms-of-service.html.

A free trial of VMware Identity Manager can be obtained by navigating to http://www.air-watch.com/lp/vmware-identity-manager-free-trial/?cid=70150000000pg4R.

Find Out More

To learn more about VMware Identity Manager or to purchase VMware or AirWatch by VMware products, call 877-4-VMWARE (outside North America, +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller. For detailed product specifications and system requirements, refer to the product documentation.

vmware®

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