VMware Identity Manager

Product and Packaging

Identity Management for the Mobile Cloud Era

VMware Identity Manager™ is identity management for the mobile/cloud era that delivers on consumer-grade expectations like one-touch access to nearly any app, from any device, optimized with AirWatch adaptive 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 from the leader of hybrid cloud infrastructure.

Customer FAQs

Q. What is VMware Identity Manager?

A. VMware Identity Manager is a service that extends your on-premises directory infrastructure to provide a seamless Single Sign-On (SSO) experience to Web, Mobile, SaaS, and legacy applications that may be consumed as a service or downloaded and installed on premises. Identity Manager integrates with AirWatch® Enterprise Mobility Management™ to enable the industry-first seamless SSO to native mobile apps and comes complete with an enterprise app store, SAML identity provider (IDP), application usage analytics, conditional access policy engine, and more.

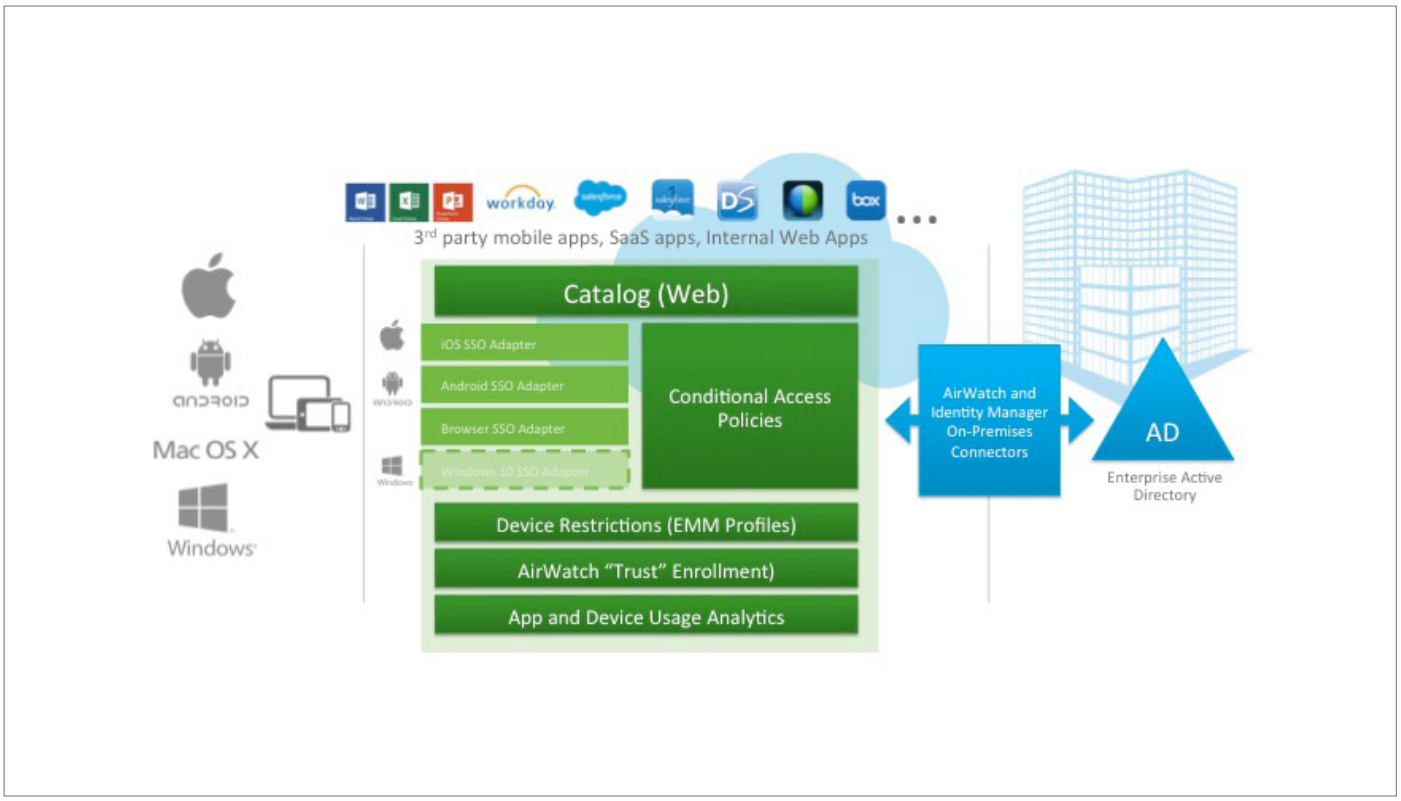

Figure 1: Product Architecture (VMware Identity Manager and AirWatch Management Suite)

Q. What are the key use cases for Identity Manager?

A. VMware Identity Manager supports two horizontal solutions today:

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. Although 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 creates compliance and security risks because IT do not have full visibility on what employees have access to, what apps or what data might be saved, and whether corporate data are 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 laptops and the respective native mobile apps for iOS, Android, and Windows 10. Although they may already be licensed to take advantage of all Office 365 has to offer, Office 365 uses a completely separate Azure Active Directory. Synchronization between Microsoft Azure Active Directory and enterprise complex on-premises active directory infrastructure proves too challenging. VMware Identity Manager federates the existing on-premises active directory to maintain one source of truth and accelerate deployment.

Q. How do I get VMware Identity Manager?

A. VMware Identity Manager Advanced Edition is available as part of the AirWatch Blue and Yellow Management Suites or through a standalone license. It is available both as a shared-cloud subscription, and as an on-premises product. VMware Identity Manager Standard Edition is only available as a part of VMware Horizon® 6 Advanced and Enterprise.

Q. How many editions of VMware Identity Manager are there?

A. There are two editions of VMware Identity Manager. The Standard Edition is available as an on-premises product only and provides the same functionality as Workspace Portal does today. The VMware Identity Manager Standard Edition will replace VMware Workspace™ Portal in the Horizon 6 Advanced and Enterprise editions. After December 31, 2015 there will no longer be a standalone SKU for Workspace Portal, but customers of the standalone product may extend existing deployments by adding the new VMware Identity Manager Advanced Edition licenses.

VMware Identity Manager Advanced Edition will include the AirWatch console for device registration. AirWatch device registration permits mobile devices and Windows 10 laptops to provide a seamless one-touch single sign-on experience for both SaaS and native mobile or Windows Metro apps.

Q. If I already have an Identity Provider or portal solution like Ping or Okta, can I still benefit from VMware Identity Manager?

A. Yes, VMware Identity Manager uniquely integrates with AirWatch to provide native mobile single sign-on and conditional access policies based on device types and whether the device is managed or unmanaged. VMware Identity Manager can interoperate with existing IDPs for SaaS apps while still presenting a common app catalog to users on browsers or mobile devices.

Q. What is the on-premises connector? Do I need this for the Identity Managercloud service?

A. Yes, while the Identity Manager cloud hosted service operates in the cloud, an on-premises connector is required to synchronize users and groups to the on premises Active Directory.

Q. Is Workspace Portal still available?

A. Yes, VMware Workspace Portal is still available both as a standalone product and bundled with Horizon Advanced and Enterprise editions. Workspace Portal is only delivered as an on-premises product. Workspace Portal will transition to VMware Identity Manager.

Q. What is the difference between VMware Identity Manager and Workspace Portal, or Horizon App Manager?

A. The core technology behind VMware Identity Manager has evolved over the past three years from Horizon App Manager and later to Workspace Portal. In fact, the architecture was originally designed as a multi-tenant cloud service, but initially delivered only as an on-premises product. The new VMware Identity Manager is the next generation of this service, integrated with AirWatch Enterprise Mobility Management, and now offered as an Identity as a Service (IDaaS) product built on top of VMware vCloud® Air™. VMware Identity Manager is delivered as an on-premises product built from the same code base as the cloud service and will replace Workspace Portal.

Q. If I have Workspace Portal today as a standalone license or purchased through Horizon Advanced or Enterprise, Do I get VMware Identity Manager?

A. Customers who are current on SnS will be entitled to future VMware Identity Manager on-premises releases as the Workspace Portal Product transitions to VMware Identity Manager. Customers who desire the new SaaS service must purchase new licenses of AirWatch Blue or Yellow Management Suites.

Q. How is VMware Identity Manager Licensed with AirWatch Management Suites?

A. VMware Identity Manager is licensed as part of AirWatch Blue and Yellow Management Suites. When purchasing device licenses, VMware Identity Manager may only be used with as many users as licensed devices. User licenses are limited to a single user. VMware Identity Manager is also included as part of VMware Workspace™ Suite.

Q. Where is the Hosted Service Offered/Located?

A. VMware Identity Manager is available as a service hosted in North America, the European Union and Asia Pacific regions. VMware Identity Manager instances leverage vCloud Air in redundant data centers for 99.9% SLA availability

Q. We own AirWatch Blue or Yellow licenses today. Will we have access to VMware Identity Manager?

A. Existing AirWatch Blue and Yellow customers may have access to VMware Identity Manager after agreeing to a revised EULA. An email will be sent to customers soon after launch to provide instructions for how to agree to the new EULA and obtain the software/service. Customers that have a license for the on-premises version of AirWatch Blue or Yellow will receive the on-premises version of the product. Customers with a shared-cloud subscription of AirWatch Blue or Yellow will receive the shared-cloud service version of VMware Identity manager. Customers with a dedicated cloud subscription will not yet have access to the VMware Identity Manager service as we do not yet support dedicated instances. Dedicated cloud customers should contact their AirWatch partner or sales representative for information.

Q. What are the system requirements for VMware Identity Manager?

A. Whether deploying VMware Identity Manager on-premises or consuming the cloud service, an on-premises connector is required to synchronize user information between Active Directory and the VMware Identity Manager service. This on-premises connector is deployed as a virtual appliance and requires a VMware vSphere® server and vCenter™ for management. For environments without existing VMware infrastructure, a vSphere Essentials license is all that is required and is backed by extensive resources and support that make it quite simple to setup.

Q. How can I purchase VMware Identity Manager?

A. VMware Identity Manger is available in two editions (Standard and Advanced). VMware customers have four options for purchasing Identity Manager (three options available via AirWatch and one option via Horizon). VMware Identity Manager Standard Edition is automatically included in the Horizon 6 Application Management Bundle. VMware Identity Manger Advanced Edition is available as a standalone product and also included in the AirWatch Blue and Yellow Management Suites.

Q. Can I upgrade from AirWatch Blue and Yellow per-device to per-user for both on-premises and cloud deployments?

A. Yes. Existing AirWatch Blue and Yellow per device customers can upgrade to per-user licensing for both type of deployments.

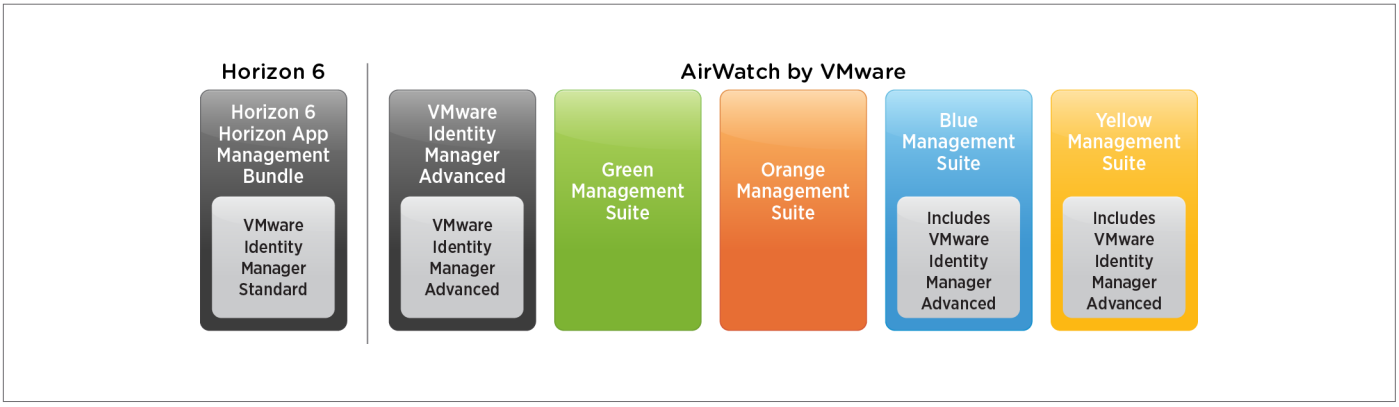

Figure 2: Available version of VMware Identity Manager

Q. Can I mix Identity Manager Advanced per-user licensing with other AirWatch per-device licensing Bundles?

A. Yes. You can add Identity Manager Advanced per user licensing to a new and/or existing AirWatch per device licensed deployment.

Q. Can I buy perpetual licenses and host VMware Identity Manager in the AirWatch cloud with hosting fees?

A. No. There is no perpetual hosting model for VMware Identity Manager Advanced for AirWatch cloud management deployments.

Q. Why does AirWatch recommend I purchase user based licensing for Identity Manager use cases for AirWatch Blue and Yellow Bundles?

A. VMware highly recommends per user licensing for customers using VMware Identity Manager.

VMware Identity Manager handles all application authentication attempts for applications that are added to the Identity Manager catalog. Therefore, if you're utilizing device-based licenses, all devices accessing applications will consume a device license. This would require an administrator to procure enough device licenses to cover all devices that could potentially access Identity Managed applications in a per-device deployment.

Scenarios

- A deployed application that is only accessible on mobile operating systems (iOS, Android, Windows 10) but restricted to authorized devices will require that per-device licenses equal the amount of authorized devices within the organization.
- A Web application that is accessed from a device that is not an authorized device (Example: User launches web app from a Chromebook.) will still consume a device license. Therefore every device that can access the Web application (authorized and unauthorized) would require a device license. Note: Web apps cannot be restricted to enrolled devices.

Opting for per-user licensing with Identity Manager provides an unlimited number of devices per user. This allows Identity Management users to utilize secure access from an unlimited amount of scenarios, including but not limited to authorized mobile devices, Chromebooks, managed PCs, unmanaged PCs, and/or BYO devices. This allows Identity Management deployments to unify and streamline the application access experience for all of your applications, on all of your devices.

Q. Will Smart Groups and Advanced Registration work in a mixed environment?

A. Yes. This is a requirement when using Identity Manager for a subset of devices that need to be managed separately within an AirWatch deployment. Identity Manager Advanced standalone licenses can be added to an existing AirWatch Blue and Yellow instance.

Q. Can I deploy Identity Manager Standard and Identity Manager Advanced in the same environment?

A. Yes. Both Identity Manager Standard and Advanced can be deployed and utilized from the same instance.

Q. Can I upgrade from Identity Manager Standard to Identity Manager Advanced?

A. No. There is no upgrade path from Identity Manager Standard to Identity Manager Advanced.

Q. Can I mix per-user and per-device licensing?

A. Yes. You can mix per-user and per-device licensing. For example: customers can deploy AirWatch Blue per-device with VMware Identity Manager Advanced per-user.

vmware

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