TOP TECH TIPS FOR IMPLEMENTING AN IDENTITY-DEFINED WORKSPACE

The global mobile workforce is set to increase from 1.32 billion in 2014, to 1.75 billion in 2020[1]. Today's increasingly mobile workers rely on a variety of devices and applications to accomplish tasks—via desktops, smartphones, tablets, or machine and enterprise Internet-of-Things (IoT) appliances. And employees want to regularly log in and out of legacy, desktop, mobile, software-as-a-service (SaaS), and cloud applications depending on the opportunity, the style of interaction, or the best set of tools for the task at hand.

The most successful digital workspace will integrate information architecture, bringing together a simple experience for end users—driven by individual identity and context at each point in time when they access an application. Identity matters in today's mobile world because there is no longer a tie to a single device or network. It's not just about an individual having a single domain login and being granted all-access. The mobile reality means work no longer happens solely on the corporate network. IT can't simply put a firewall in front of the data center. Companies need to build a new security perimeter around the user to remove the obstacles that prevent working any time and any place. Today, almost every app and every service may require a unique authentication.

WHAT IS VMWARE WORKSPACE ONE?

VMware Workspace™ ONE™ combines identity and mobility management to provide frictionless and secure access to all the apps and data employees need to work, wherever, whenever, and from whatever device they choose. To learn more about Workspace ONE, visit https://workspaceone.com.

It is up to enterprises to meet these needs and embrace digital transformation; it's good for users and good for business. With this in mind, here are the top technical tips to help you make your VMware Workspace ONE deployment the pinnacle platform for your identity-defined workspace:

1. Enable seamless access to apps and data across devices

Using Salesforce as an example, this can be easily accomplished by providing a single sign-on (SSO) to the Salesforce Web application on the user's corporate desktop, corporate laptop, as well as their personal PC via the Workspace ONE Web portal and via a corporate-managed or "bring your own" (BYO) mobile device through delivery and configuration of the native mobile Salesforce application.

2. Ensure data on BYO devices remains secure no matter the employee's status

End users expect companies to deliver applications, desktops, and mobile applications to whatever device they choose, including BYO mobile iOS and Android devices. However, there remains the obvious need to ensure data on BYO mobile devices is still secure and capable of being wiped from the user's device if they leave the company or lose the device.

Workspace ONE has the ability to adaptively manage and enroll devices as needed when the end user needs additional access. When the end user just needs access to corporate basic applications, they can simply log in via Workspace ONE and authenticate via Workspace ONE single sign-on. When more secure application access is needed, Workspace ONE can push enrollment of the device for corporate data and application management to ensure the corporate data is secure. If the device is lost, or the user leaves the company, data can simply be removed by un-enrollment (requested by the user or by corporate IT) without affecting anything else on the end user's mobile device.

1 Strategy Analytics. "Global Mobile Workforce Forecast, 2015-2020," November 3, 2015.

3. Allow end users to easily log in while still maintaining security

Many end users are understandably resistant to complex configurations and multi-touch authentication such as RSA SecurID and other token authentication methods from their mobile devices (including laptops, tablets, and smartphones). Workspace ONE, through the use of VMware Identity Manager™ secure app token and multi-factor authentication features and VMware Verify, can provide both easy-to-use single sign-on functionality along with the use of multi-factor authentication if needed.

The secure app token feature uses a variety of technologies for the various platforms (for example, Cloud KDC for iOS, Android for Work and Chrome Tabs for Android, and Windows Account Provider and TBAUTH).

4. Consolidate the number of digital identities by integrating with third-party identity providers

Third-party identity providers (IdPs) such as Ping can be configured with VMware Identity Manager to "daisy-chain" end-user authentications. For example, Ping would be the IdP for Salesforce, serving as the service provider. To chain these via VMware Identity Manager, Identity Manager becomes the IdP for Ping and Ping acts as the service provider.

Sample workflow:

1. Request from Salesforce sent to Ping.
2. Ping makes a policy decision based on user, application, desktop vs. mobile, and more.
3. Ping adapter authenticates the desktop user.
4. Ping forwards mobile request to VMware Identity Manager.
5. VMware Identity Manager makes a policy decision.
6. Device authenticates with mobile authentication endpoint.
7. Redirect back to Ping.
8. Ping issues a SAML assertion to Salesforce.
9. Success.

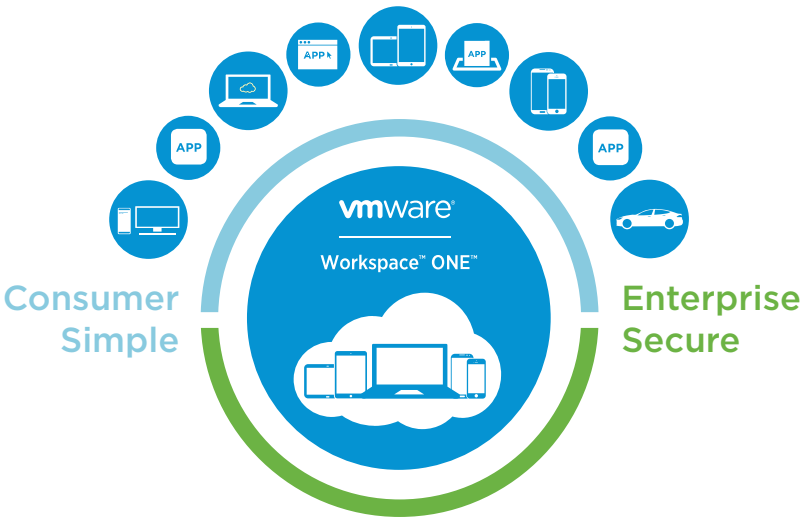
5. Ease external enterprise system integrations via connectors

Both the VMware AirWatch® Cloud Connector™ and VMware Identity Manager Connector enable single-sign-on authentication for end users. How this is accomplished is unique to the individual connectors.

AirWatch Cloud Connector (ACC) – Consider using the ACC when using a SaaS identity manager tenant, or when you have the need for a single sign-on into SaaS, Web-based applications, or mobile applications.

This synchronizes users from the local Active Directory into the VMware AirWatch tenant. The AirWatch tenant synchronizes these users and groups into VMware Identity Manager for user authentication into Workspace ONE. The ACC only requires an outbound TCP 443 connection.

Two things are paramount for success: Consumer simplicity and enterprise security.



VMware Identity Manager Connector – Consider using the VMware Identity Manager Connector when deploying the on-premises offering of VMware Identity Manager, or if you require integration of the Identity Manager SaaS tenant with VMware Horizon®, VMware ThinApp®, or Citrix XenApp and XenDesktop environments for single sign-on into environments in conjunction with SaaS and/or Web-based applications.

This synchronizes users from the local Active Directory into the VMware Identity Manager tenant. The Identity Manager Connector will support an "outbound only" communication model using only TCP 443 outbound to communicate with the SaaS identity manager tenant when using the requisite cloud-deployment authentication methods such as a password, RSA Adaptive Authentication, RSA SecurID, or Remote Authentication Dial-In User Service (RADIUS). Additional authentication adapters such as Kerberos (KerberosIdpAdapter) will still require TCP 443 inbound connectivity which uses an external, public Network Address Translated IP address and a public fully qualified domain name (FQDN) for the on-premises VMware Identity Manager Connector. Additionally, the on-premises offering of VMware Identity Manager automatically deploys the connector within a single virtual appliance (SVA).

Both – If both mobile applications (as well as integration with VMware Horizon, ThinApp, or Citrix XenApp and XenDesktop environments) are needed, then both the VMware AirWatch Cloud Connector and VMware Identity Manager Connector are needed.

Note: Workspace ONE supports all configurations of SaaS and Web applications.

Why Embrace an Identity-Defined Workspace?

- Federates identity for on-premises and cloud services.
- Removes friction from the user experience.
- Provides contextual rules-engine with continuous security.
- Allows access by default.
- Enables a single clearinghouse for entitlement and authentication.
- Verifies device posture for compliance.

ABOUT VMWARE IDENTITY MANAGER

VMware Identity Manager is an Identity as a Service (IDaaS) offering, providing application provisioning, self-service catalog, conditional access controls, and single sign-on for SaaS, Web, cloud, and native mobile applications.

Benefits include:

- Simplify business mobility with one touch from any device
- Optimize user experience and security with VMware AirWatch
- Empower employees with a self-service app store
- Trusted VMware enterprise-grade hybrid cloud infrastructure

For more information on VMware Identity Manager, visit http://www.vmware.com/products/identity-manager.html.

Conclusion

With a digital workspace, people can use any desktop or device—BYO or corporate-owned—at any time while IT administrators safely automate application distribution and updates on the fly. Enterprises that deploy an identity-defined workspace can easily embrace heterogeneity because identity access and personalization transcends every application, across every device.

VMware Workspace ONE is a platform set containing solutions such as VMware AirWatch®, Socialcast™ by VMware, VMware Horizon Enterprise Edition, ThinApp, VMware User Environment Manager™, VMware App Volumes™, and VMware Identity Manager.

In fact, VMware Identity Manager is the underlying support for the entire Workspace ONE solution, providing the glue to bring all of these products and solutions together under the Workspace ONE umbrella. VMware Identity Manager also provides a single-sign-on experience for end users into all of their remote services, desktops, and applications—including legacy Windows applications, hosted and remote applications and desktops (including Citrix), SaaS- and Web-based applications, as well as mobile apps, content, and device management.

Test-drive Workspace ONE and have it up and running on your browser in minutes, with no installation required. Check out the Hands-On Lab now.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 7509-VMW-TT-IDDEFWORKSPACE-USLTR-WEB
09/16