VMware Workspace ONE Access

AT A GLANCE:

VMware Workspace ONE® Access™ delivers multifactor authentication (MFA), conditional access and single sign-on (SSO) for applications delivered by VMware Workspace ONE. By acting as a broker to other identity stores and providers, Workspace ONE Access enables organizations to quickly and more securely implement application and device strategies that deliver consistent, enterprise-wide access to applications and data from any device in any location.

In increasingly heterogeneous IT environments, the user's identity is the constant. VMware Workspace ONE Access (formerly VMware Identity Manager) combines the user's identity with factors such as device and network information to make intelligence-driven, conditional access decisions for applications delivered by Workspace ONE. This enables organizations to quickly and more securely provide a consistent application access experience from any device.

Available as a cloud-hosted service, Workspace ONE Access is an integral part of the Workspace ONE platform and supports Workspace ONE Intelligent Hub, Workspace ONE Unified Endpoint Management (UEM) and VMware Horizon®. Workspace ONE Access acts as a broker to other identity stores and providers—including Active Directory (AD), Active Directory Federation Services (ADFS), Azure AD, Okta and Ping Identity—that your organization may already be using to enable authentication across on-premises, software-as-a-service (SaaS), web and native applications without the need to rearchitect the identity environment. Its capabilities help ensure your organization can deploy new applications of any type with a consistent user experience.

Key features

Access broker – Integrates with existing on-premises and cloud identity providers to reduce deployment times and enable more secure access to any application while improving user experience.

Adaptive MFA and SSO – Provides native MFA or integrates with exiting MFA providers, and delivers SSO to web, SaaS, mobile and legacy apps through integration with Workspace ONE Intelligent Hub.

Risk-based conditional access – Uses dozens of access policy combinations that leverage device enrollment, network, SSO, automated device remediation and third-party information to establish levels of trust, enabling intelligent access decisions.

Cloud-hosted option – Dramatically reduces implementation time and maintenance overhead.

Smarter digital workspace – Unlocks new Workspace ONE features and capabilities, including Workspace ONE Hub Services and Workspace ONE Intelligence, on day one without scheduling and prioritizing upgrade cycles.

Accelerating Office 365 deployments with the digital workspace

Many businesses deploy Microsoft Office 365 as the first SaaS application to every user in their organization. Yet, Office 365 is no regular application deployment. Employees want to access Office applications on their desktops and laptops, and also use native apps on their tablets and phones (iOS and Android). This raises new issues about deploying and securing Office applications and their content. As part of the Workspace ONE platform, Workspace ONE Access provides secure, conditional access to Office apps on any device. It accelerates deployment times by brokering complex AD and Azure AD environments and securing access with options, including mobile application management (MAM), device enrollment and MFA. Workspace ONE can integrate with any data loss prevention (DLP) requirements using Microsoft Graph APIs and extend these rules to non-Microsoft applications for a consistent security policy.

Taking strides to zero trust

Businesses designing an access experience for their users that truly delivers on the any device, anywhere promise are removing the perimeter and gaining a fresh approach to protecting data. Workspace ONE Access seamlessly integrates with Workspace ONE Intelligent Hub, Workspace ONE UEM and Horizon desktops and apps, providing your organization with the tools to deliver a zero-trust security model. Device, user and network information are taken into account during the authentication and authorization process. A trusted identity on a trusted device from a trusted network may only need to enter a PIN. A trusted identity on an unknown device and an untrusted network may be prompted for MFA, which requires a PIN and a biometric or a one-time token sent to a trusted phone.

Providing cloud hosting for greater IT agility and efficiency

By using Salesforce, Office 365, Workday and other enterprise applications, organizations recognize hosting complex infrastructure such as identity brokering in the cloud delivers many advantages. With Workspace ONE Access, your organization can experience:

- Fast initial setup – There's no equipment to purchase and no re-architecting of legacy environments.
- Simplified and automated deployment – Deployment of new services in days rather than months, built-in security and adherence to requirements such as SOC 2 and HIPAA help keep your business compliant and competitive.
- Worry-free maintenance and easy updates – Automatic updates with the latest security patches and VMware software protect your organization against threats.
- High availability – Automatic failover and recovery, plus a 99.9 percent uptime service-level agreement (SLA) with continuous monitoring by VMware, give you peace of mind.
- Lower CapEx and OpEx – Lower upfront expenditures and ongoing costs free your valuable IT resources to focus on innovation rather than keeping the lights on.

Getting started

VMware Workspace ONE Access is part of the Workspace ONE platform. To realize the benefits of hosted Workspace ONE Access, contact your VMware sales representative or see the solution in action with a Hands-on Lab.

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