REVIEWER'S GUIDE FOR CLOUD-BASED VMWARE WORKSPACE ONE: OVERVIEW

VMware Workspace ONE

vmware®

Table of Contents

Introduction

The *Reviewer's Guide for Cloud-Based VMware Workspace ONE: Overview* provides a comprehensive technical overview of VMware Workspace™ ONE™. Workspace ONE simplifies access to cloud, mobile, and enterprise applications from supported devices. IT administrators can deploy, manage, and secure applications and, at the same time, offer a flexible, bring-your-own-device (BYOD) option for users.

Purpose of This Guide

The Reviewer's Guide helps you evaluate Workspace ONE by offering practical exercises. This overview is first in the Reviewer's Guide series. It introduces Workspace ONE and its benefits, features, architecture, and components. For information about the other guides in the series, see All Guides.

Important: This guide is for evaluation purposes only. It uses the minimum required resources for a basic deployment and does not explore all possible features. Do not use this evaluation environment as a template for deploying a production environment. To deploy a production environment, see the VMware Workspace ONE Documentation.

Audience

This guide is for prospective IT administrators of Workspace ONE and anyone who uses the product.

VMware Workspace ONE Features

Today's workforce depends on mobility. Yet advancements in IT can challenge mobility: How can an organization support existing enterprise applications and new cloud and mobile applications while maintaining simple remote access for its end users? Workspace ONE focuses on end-user application access while meeting IT's changing enterprise security and management requirements.

Workspace ONE is an integrated platform powered by the VMware AirWatch® Enterprise Mobility Management™ service. Workspace ONE also includes VMware Identity Manager™ technology and Workspace ONE mobile applications for Android, iOS, and Windows 10.

Note: You can install the Workspace ONE mobile application for Windows 10 on any Windows 10 device. Windows 10 devices include Windows phones, Windows Surface tablets, and Windows 10 laptops and desktops. While some of these devices might not typically be considered mobile, they are treated as mobile devices for the purpose of this guide.

Workspace ONE Enterprise edition includes VMware Horizon® 7 Enterprise Edition. Horizon 7 offers flexible deployment options, including on-premises, cloud-based, and mixed implementations with some components onsite and others in the cloud.

VMware Identity Manager provides single sign-on (SSO) to an application store for software-as-a-service (SaaS)-based Horizon 7, Citrix, VMware ThinApp®, and web applications, as well as for Horizon 7 virtual desktops. VMware Identity Manager also provides a set of networking and authentication policies to control application access. VMware AirWatch provides device enrollment, application distribution, productivity tools, and compliance-checking tools to ensure that remote access devices meet corporate security standards. The Horizon 7 platform enables access to virtual desktops and applications from a range of supported devices. In addition, Workspace ONE provides an application store that presents a consistent end-user experience. This application store leverages native platform capabilities, such as biometrics or security features in the operating system, to ensure a consumer-simple, enterprise-secure means of accessing applications.

The integration of VMware Identity Manager, VMware AirWatch, and Horizon 7 enables the Workspace ONE platform to deliver the advanced mobility, security, and identity-based management that enterprises need today. Although you can implement VMware AirWatch and Horizon 7 as individual technologies, you must implement VMware Identity Manager and VMware AirWatch to deploy Workspace ONE.

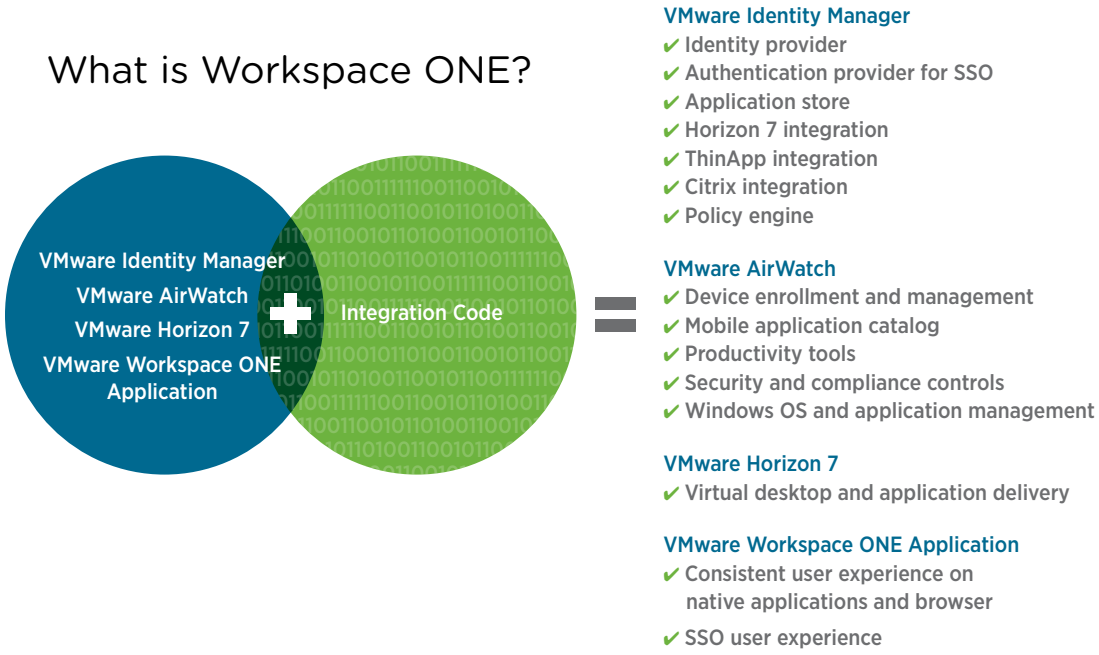

Figure 1: Workspace ONE Platform

Workspace ONE deployments can include the following BYOD options:

- **Unmanaged** – Access web and virtual applications from a web browser.
- **Managed workspace** – Choose your own device and access-approved applications. IT manages the workspace, and you manage the device.
- **Managed workspace with endpoint management** – Choose your own device, or use a corporate-issued device. IT fully controls these devices.

Features in Workspace ONE include:

- Native mobile Workspace ONE application
- Integrated application store
- Mobile SSO
- Productivity tools
- Conditional access with device compliance
- Multifactor authentication
- Windows 10 management
- Adaptive management

Native Mobile Workspace ONE Application

Users can install the Workspace ONE application on a mobile device and, using corporate credentials, get SSO access to corporate, cloud, and mobile applications.

The Workspace ONE application uses native OS capabilities to protect application access, such as biometric fingerprint readers on Android, Touch ID on iOS, and Windows Hello on Windows 10.

For more information, see the VMware Workspace ONE Documentation.

Integrated Application Store

Workspace ONE provides users access to cloud, mobile, and Windows applications using a unified application store. The application store contains applications published to VMware Identity Manager and VMware AirWatch. Supported application types include internal web, SaaS, native mobile, internally developed mobile, legacy and modern Windows, Horizon 7, VMware Horizon Cloud Service™, Citrix published, and ThinApp. The application store also contains virtualized desktops.

Using the Workspace ONE application, you access VMware Identity Manager applications from the Launcher tab and all published applications from the Catalog tab. The Workspace ONE application provides more functionality than accessing the application store from a browser, where only VMware Identity Manager applications are available.

The latest Workspace ONE release supports Spotlight Search in iOS devices. Users can search their home screen and Workspace ONE catalog at the same time.

For more information, see the VMware Workspace ONE Documentation.

Mobile SSO

Workspace ONE provides Mobile SSO, a one-touch login implementation to mobile applications using the patent-pending, secure-application token system (SATS) that establishes trust between the user, device, application, and enterprise. You can secure applications by locking a known, registered device through a PIN or biometric service. After users have provided credentials, they can touch an application to open it until the authentication window expires. Mobile SSO is available for Android, iOS, and Windows 10 devices.

For more information, see the Your Problem's Solved: Enable Secure Native Mobile App SSO on Any Device blog post and VMware Workspace ONE Documentation.

Productivity Tools

Workspace ONE includes productivity tools, such as VMware AirWatch Inbox™, VMware AirWatch Content Locker™, VMware AirWatch Browser™, and VMware Boxer™. These tools maximize user productivity while securing corporate data.

For more information, see the VMware AirWatch Documentation.

Conditional Access with Device Compliance

Workspace ONE allows you to configure network, platform, and application-specific criteria for authentication. A device must prove compliance with security rules prior to authorizing access to an application. Compliance rules protect against rooted or jailbroken devices, and you can use them to whitelist and blacklist applications.

For more information, see the VMware Workspace ONE Documentation.

Multifactor Authentication

Workspace ONE, integrated with the mobile application VMware Verify™, provides strong, multifactor authentication that simplifies access across devices. When a user attempts to access the Workspace ONE application store, or any application requiring strong authentication, VMware Verify sends a notification to the user's mobile phone. To verify attempted access to Workspace ONE and launch the application, the user must swipe **Accept**.

For more information, see the VMware Workspace ONE Documentation.

Windows 10 Management

Workspace ONE takes full advantage of Windows 10 management capabilities and simplifies the application and device life cycle.

Using Workspace ONE with VMware AirWatch eliminates the need for laptop imaging. IT can remotely configure, manage, and monitor devices in any location. Management configurations are based on dynamic smart groups, which consider device information and user attributes, and are automatically updated as that information changes.

You can use VMware AirWatch to automatically install, update, and remove software packages. It also provides scripting and file management tools. You can configure packages to install based on conditions, including network status or defined schedules, deploy software updates automatically, and notify users when updates occur.

For more information, see the VMware Workspace ONE Documentation.

Adaptive Management

For applications that require only a basic level of security, users are not required to enroll their device into VMware AirWatch Mobile Device Management™. Users can download the Workspace ONE mobile application and select the applications they want to install. For applications that require a higher level of security, users can enroll their device into VMware AirWatch directly from the Workspace ONE mobile application instead of through VMware AirWatch Agent™.

All entitled applications are listed in the catalog. Applications that require enrollment are indicated with a lock icon. When the user tries to download an application with a lock icon, the enrollment process is triggered. For example, users can download a conferencing application, such as WebEx, without enrollment. But they are prompted to enroll when they try to download an enterprise application, such as Salesforce.

For more information, see the VMware Workspace ONE Documentation.

Packaging and Licensing

All Workspace ONE editions are licensed on a per-named-user basis and available as an annual cloud subscription or a perpetual on-premises license.

For more information, see *VMware Workspace ONE* in the VMware Workspace ONE and VMware Horizon Packaging and Licensing guide.

Workspace ONE Architecture and Components

This section provides a general overview of Workspace ONE and its components and architecture.

How Workspace ONE Works

IT can deploy Workspace ONE in many different configurations. Options include on-premises deployments of VMware Identity Manager and VMware AirWatch, cloud-based deployments of VMware Identity Manager and VMware AirWatch, and hybrid deployments with different components available either on-premises or in the cloud.

Whichever deployment you choose, you can configure Workspace ONE to use an existing directory infrastructure, such as Active Directory or other LDAP-based directory, for user synchronization, authentication, and application access.

Administrators choose which applications to deploy and make them available from the VMware Identity Manager and VMware AirWatch Console.

Administrators create a unified catalog by configuring VMware Identity Manager with the VMware AirWatch instance. Configuring Workspace ONE involves creating a trusted relationship between the VMware Identity Manager and the VMware AirWatch implementations through their respective consoles. Each console is used to configure the relevant platform capabilities.

Workspace ONE supports one-touch login that can be used by Android, iOS 9 and later, and Windows 10 devices. One-touch login establishes trust between the user, device, and enterprise for one-touch authentication. For more sensitive applications, IT can enable biometric or other multifactor authentication methods.

In a traditional IT environment, you can prevent data leakage in a number of ways. Examples of data leakage include saving work documents to public storage, such as Dropbox, or receiving work emails in an unmanaged email client. You can encrypt email attachments and restrict how the files are edited and shared. You can require using corporate-approved applications instead of native applications. For secure browsing, you can enable access to intranet sites to ensure that the sites are opened only in approved browsers. However, these precautions might be insufficient for your security needs.

For increased security, you can enforce granular control of devices with Workspace ONE compliance checking, which combines VMware AirWatch device-based rules and VMware Identity Manager user-based identity rules. A user cannot access applications with a device unless the device adheres to the security rules applied. For example, you can deny application access based on the operating system (OS) or patch level of the device, if the device has been jailbroken, or if the device is in a foreign country.

IT can use mobile OS management interfaces to preconfigure laptops, smartphones, and tablets. VMware AirWatch device management uses enterprise mobile management APIs to provision, configure, and secure applications and devices. For example, you can configure supported devices to receive patches directly from the OS vendor. This level of control allows IT to adopt a flexible BYOD program by giving users device choice while securing data.

Windows 10 management capabilities allow desktop administrators to automate application delivery and updates. For example, IT can streamline how updates are managed and delivered by letting users control OS updates or enforcing them with Windows Update or Windows Update for Business. IT can also get users operational quickly by bulk-enrolling devices and delivering complete Windows provisioning packages for users to install with one click.

Administrators create VMware AirWatch device profiles based on criteria such as users, groups, platforms, and OS, and assign profiles to *smart groups*.

Using adaptive-management technologies, users can install the Workspace ONE mobile application from the application store for their platform and log in with their corporate credentials giving them access to their authorized applications in the catalog. If users need access to more privileged applications, they can be prompted to enroll their device into full VMware AirWatch management. Based on the device profile assigned, the VMware Identity Manager catalog displays all entitled applications, including mobile applications, SaaS applications, and Horizon 7–based virtual applications and desktops. The applications that require enrollment have a badge indicating higher security.

A Workspace ONE implementation can interoperate with other identity providers, like Ping, Okta, and Microsoft Azure, through integration with VMware Identity Manager and still present a common catalog interface for all applications.

Workspace ONE Architecture

A basic Workspace ONE configuration consists of VMware Identity Manager and VMware AirWatch. VMware Enterprise Systems Connector™ securely transmits requests from VMware AirWatch to the back-end infrastructure. Administrators define user groups, policy settings, and device configurations. Users access Workspace ONE and their applications based on the defined settings and configurations.

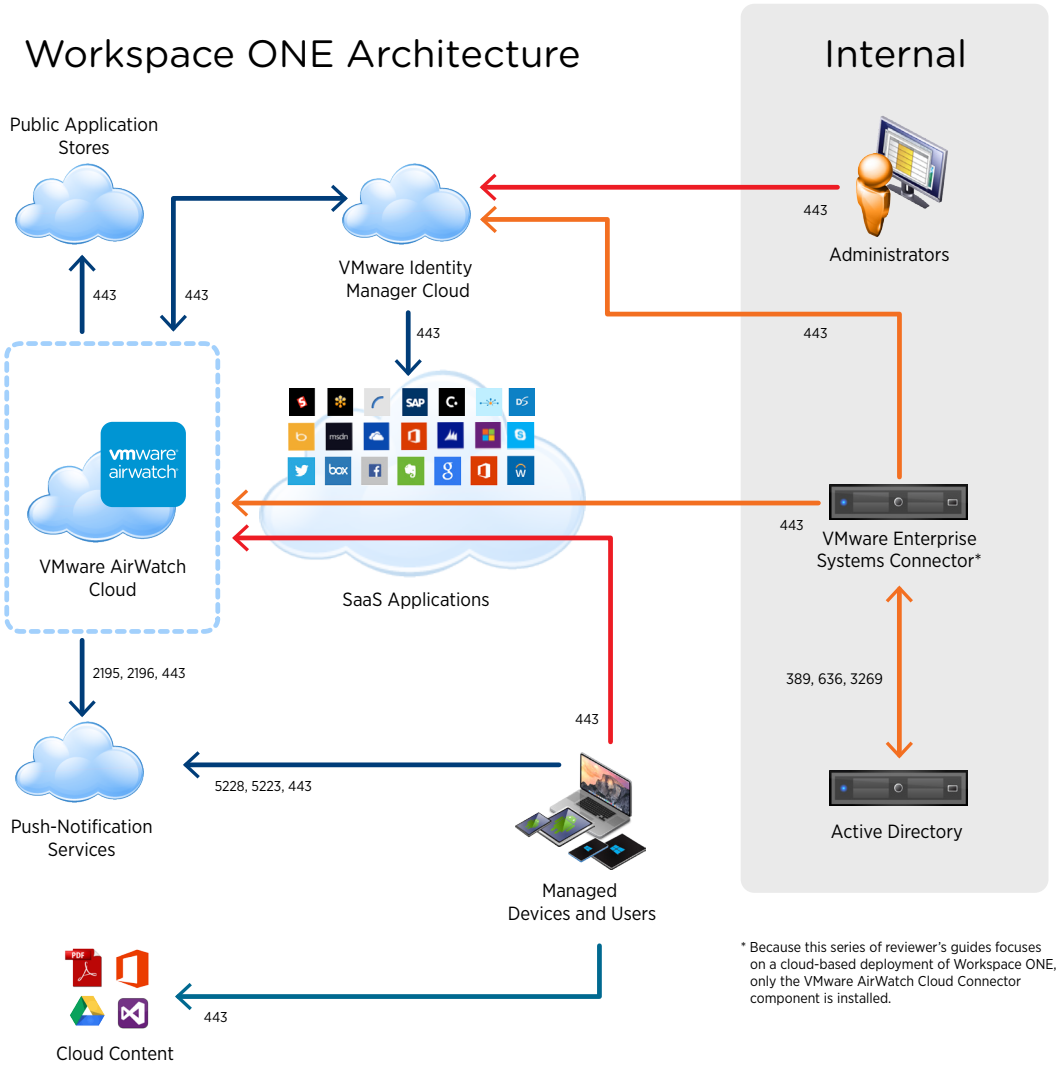

Figure 2: Major Components of a Workspace ONE Deployment with Network Ports

Network Considerations

VMware AirWatch leverages the existing enterprise network infrastructure to provide its own high availability, redundancy, and scalability for the applications and desktops that it provides to end users. Local load balancing is incorporated on the front end of the SaaS environment. Core network security infrastructure includes redundant Ethernet switches, LAN segregation, firewalls, intrusion detection, and monitoring.

Redundant, high-volume firewalls are located between the Internet and the VMware AirWatch environment. An intrusion detection system (IDS) monitors all internal network traffic, logs suspicious activity, and issues alerts when suspicious network activity is detected.

Security Considerations

VMware AirWatch takes a multilayered approach to data center security. Primary data centers are maintained with onsite backups for quick recovery and replicated offsite backups for disaster recovery.

Production systems are hosted at two primary data centers, with cross replication of nightly backups to support performance, growth, and security challenges.

VMware AirWatch implements security by

- Isolating all VMware AirWatch web servers using a demilitarized zone (DMZ)
- Using antivirus clients to protect all servers
- Providing spam filtering and spam reporting for email

Administrators control VMware AirWatch from an HTML5 web-based management console. VMware AirWatch encrypts all data transmitted between the web console and mobile devices.

Cloud-based Workspace ONE components are automatically upgraded and patched, ensuring that your environment meets the latest security standards.

Workspace ONE Components

Workspace ONE consists of a number of key components and integrations:

- VMware Identity Manager
- VMware AirWatch
- VMware Horizon 7
- Workspace ONE native application
- VMware Enterprise Systems Connector
- VMware Identity Manager administration console
- VMware Unified Access Gateway
- VMware AirWatch Secure Email Gateway
- VMware AirWatch console
- VMware AirWatch Inbox
- VMware AirWatch Content Locker
- VMware AirWatch Browser
- VMware Boxer

VMware Identity Manager

VMware Identity Manager is an identity-as-a-service (IDaaS) offering, providing application provisioning, an application store, conditional access controls, and SSO for SaaS, web, cloud, and native mobile applications.

For more information, see the VMware Identity Manager Documentation.

VMware AirWatch

VMware AirWatch is a comprehensive enterprise mobility platform that delivers simplified access to enterprise applications, secures corporate data, and enables mobile productivity. The VMware AirWatch family includes individual VMware AirWatch products.

For more information, see the VMware AirWatch Documentation.

VMware Horizon 7

Horizon 7 allows you to deliver virtual and hosted desktops and applications through a single platform.

For more information, see the VMware Horizon 7 Documentation.

Workspace ONE Native Application

You can install the Workspace ONE native application on Android, iOS, and Windows 10 devices. It allows users to access their digital workspace from any supported location.

For more information, see the VMware Workspace ONE Documentation.

VMware Enterprise Systems Connector

In VMware AirWatch 9.1, the VMware AirWatch Cloud Connector™ and VMware Identity Manager connector are included as components in a new Windows installer called the VMware Enterprise Systems Connector. During the installation process, you can choose which components to install. It is recommended to install both components if you are upgrading to Workspace ONE and for full functionality of the Enterprise Systems Connector.

The VMware Identity Manager connector allows Active Directory (or other directory services) users and groups to synchronize with VMware Identity Manager and provide up-to-date authentication. The VMware Identity Manager connector supports integration with Horizon 7 and Citrix, RSA Secure ID, Windows authentication, and complex multi-domain and multi-forest Active Directory.

AirWatch Cloud Connector allows you to integrate VMware AirWatch with your back-end enterprise systems. AirWatch Cloud Connector runs in the internal network, acting as a proxy that securely transmits requests from VMware AirWatch to your organization's critical enterprise infrastructure components. AirWatch Cloud Connector leverages the benefits of AirWatch Enterprise Mobility Management, installed on-premises or in the cloud, together with Active Directory (or other directory services), certificate authorities, email servers, and other internal systems.

For more information, see the VMware Workspace ONE Documentation.

VMware Identity Manager Administration Console

The VMware Identity Manager administration console is a web-based application for managing your cloud instance, or *tenant*.

For more information, see the VMware Identity Manager Documentation.

VMware Unified Access Gateway

VMware Unified Access Gateway secures external access to internal content. Users can remotely access data from corporate network shares or internal content repositories. Updates to your existing content are dynamic. Changes are immediately reflected in AirWatch Content Locker. Users can access only the files and folders that have been assigned to them through access control lists.

VMware Tunnel™ is deployed using the Unified Access Gateway appliance and provides a secure and effective method for individual applications to access corporate resources. VMware Tunnel authenticates and encrypts traffic from individual applications on supported devices to the back-end system. Built using native operating system APIs, VMware Tunnel provides enhanced network security (including micro-segmentation), consistent enterprise network access for end users, and simplified management for IT.

For more information, see the VMware Unified Access Gateway Documentation.

VMware AirWatch Secure Email Gateway

VMware AirWatch Secure Email Gateway™ is a proxy server that is configured with AirWatch Mobile Email Management features to protect your email infrastructure. When AirWatch Secure Email Gateway is installed alongside your existing email server, it proxies all email traffic to enrolled devices. Based on settings defined in AirWatch Console, AirWatch Secure Email Gateway allows or blocks requests from every mobile device it manages. It filters all communication requests and relays traffic from approved devices, thereby protecting corporate email servers. Users can open email attachments only through AirWatch Content Locker and access hyperlinks contained in email messages only through AirWatch Browser, thus securing sensitive information.

For more information, see the VMware AirWatch Documentation.

VMware AirWatch Console

VMware AirWatch Console is a web-based application that allows you to monitor and manage enrolled devices.

For more information, see the VMware AirWatch Documentation.

VMware AirWatch Inbox

AirWatch Inbox is a containerized email client protected with 256-bit AES encryption. (In this context, *containerized* means that content in the email application is isolated from content in other applications on the device.) It is configured with data-loss-prevention capabilities to secure corporate data and allows for quick access to corporate email, calendars, and contacts.

For more information, see the VMware AirWatch Documentation.

VMware AirWatch Content Locker

AirWatch Content Locker protects your sensitive content in a corporate container and provides users with a central application to securely access, store, update, and distribute the latest documents from their mobile devices.

For more information, see the VMware AirWatch Documentation.

VMware AirWatch Browser

AirWatch Browser provides a secure alternative to the native browsers on mobile operating systems. You can secure all Internet browsing and limit browsing to certain websites.

For more information, see the VMware AirWatch Documentation.

VMware Boxer

VMware Boxer is an integrated mail, calendar, and contacts application for VMware AirWatch and Workspace ONE mobile users. It allows IT to configure and manage security policies at a granular level. Some features include the ability to select multiple email messages and perform a single task, such as delete, archive, or flag, compose an email message, and send available calendar times in just a few taps.

For more information, see the VMware AirWatch Documentation.

Summary

This overview starts the *Reviewer's Guide for Cloud-Based VMware Workspace ONE* series. It describes the architecture of Workspace ONE and its individual components and their interoperability. For information about the other guides in the series, see All Guides.

All Guides

You can explore many key features and capabilities in the Reviewer's Guide series for cloud-based Workspace ONE:

- Reviewer's Guide for Cloud-Based VMware Workspace ONE: Overview
- Reviewer's Guide for Cloud-Based VMware Workspace ONE: VMware Systems Enterprise Connector Installation and Configuration
- Reviewer's Guide for Cloud-Based VMware Workspace ONE: Mobile SSO

Note: For information about features that are not covered in this series, see the VMware Workspace ONE Documentation.

Appendix: Terminology Used in This Guide

The following terms are used in this guide.

application store	A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.
catalog	A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.
cloud	A set of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.
device enrollment	The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.
identity provider (IdP)	A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.
mobile device management (MDM) agent	Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the VMware Glossary.

Additional Resources

For more information about Workspace ONE, you can explore the following resources.

- VMware Workspace ONE Product Page
- VMware Workspace ONE Documentation
- VMware Identity Manager Product Page
- VMware Identity Manager Documentation
- VMware AirWatch Product Page
- VMware AirWatch Documentation
- VMware Workspace ONE free trial
- VMware Workspace ONE Enterprise Edition Reference Architecture
- VMware End-User-Computing Blog
- Workspace ONE Hands-On Lab

About the Authors and Contributors

The *Reviewer's Guide for Cloud-Based VMware Workspace ONE* was written and updated by

- Gina Daly, Technical Marketing Manager in End-User-Computing Technical Marketing, VMware
- Kevin Sheehan, Senior Product Manager, Windows 10 Unified Endpoint Management, VMware

Appreciation and acknowledgment for considerable contributions from the following subject matter experts:

- Camilo Lotero, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware
- Justin Sheets, Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

Contributors to this version include

- Andrew Hornsby, Product Manager, Mobile Identity, VMware
- Vikas Jain, Director, Product Management, VMware Workspace ONE, VMware
- Ben Siler, Product Marketing Manager, VMware Workspace ONE, VMware

Contributors to the original document include

- Oliver Forder, Lead End-User-Computing Specialist, EMEA End-User-Computing Practice, VMware
- Neil Tarbit, Director, Systems Engineering, End-User Computing, VMware
- Roger Deane, Senior Manager, End-User-Computing Technical Marketing, VMware
- Hannah Jernigan, Technical Marketing Manager, End-User-Computing Technical Marketing, VMware

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

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