

Workspace ONE Deploy and Manage

AT-A-GLANCE

The Workspace ONE Deploy and Manage course teaches you fundamental techniques to implement WorkspaceONE UEM effectively.

TARGET AUDIENCE

- Systems Engineers
- Consulting Architects
- Microsoft End-User Computing Specialists

DELIVERY METHOD

- Instructor-led, classroom-based
- Live Online
- Private Training

COURSE DURATION

Five (5) days of instructor-led classroom training

PREREQUISITES

- This course has no Prerequisites

AVAILABILITY

This course is being offered through the Omnissa learning platform.

TECHNICAL REQUIREMENTS

- Please ensure you have the US keyboard mapping added to your devices.

Course Overview

In this five-day course, you learn how to apply the fundamental techniques for launching and maintaining an intelligence-driven, multi-platform endpoint management solution with Omnissa Workspace ONE® UEM. Through a combination of hands-on labs, simulations, and interactive lectures, you will configure and manage the endpoint life cycle.

Course Objectives

You will learn to apply the fundamental techniques for integrating Omnissa Workspace ONE® Access™ with Workspace ONE UEM to securely distribute business-critical applications and configure access management controls from any device. Through a combination of hands-on labs, simulations, and interactive lectures, you configure enterprise, productivity, and Omnissa Access integrations.

This course lays out the principles of identity and access management. You will leave with a fundamental understanding of how Workspace ONE uses various authentication methods and protocols to determine user access permissions and enable single sign-on.

By the end of this session, attendees should be able to:

- Explain and apply the fundamental techniques for launching and maintaining an intelligence-driven, multiplatform endpoint management solution with Workspace ONE UEM
- Outline the components of Workspace ONE UEM
- Explain the general features and functionality enabled with Workspace ONE UEM
- Summarize basic Workspace ONE administrative functions
- Explain and deploy common Workspace ONE integrations
- Securely deploy configurations to Workspace ONE UEM managed devices
- Onboard device endpoints into Workspace ONE UEM
- Summarize alternative management methodologies for rugged devices
- Discuss strategies to maintain environment and device fleet health
- Configure and deploy applications to Workspace ONE UEM managed devices
- Analyze Workspace ONE UEM deployments
- Enable email access on devices
- Integrate Workspace ONE UEM with content repositories and corporate file shares
- Explain the general features and functionality that Omnissa Access enables
- Summarize and implement Workspace ONE productivity services into the digital workspace environment

Course Modules

1. Course Introduction

- Introductions and course logistics
- Course objectives

2. Platform Architecture

- Summarize the features and functionality of Workspace ONE UEM
- Outline the benefits of leveraging Workspace ONE UEM
- Recognize the core and productivity components that make up the Workspace ONE UEM platform
- Summarize high availability and disaster recovery for Workspace ONE Solution

3. Administration

- Navigate and customize the Workspace ONE UEM console
- Summarize the hierarchical management structure
- Explain the features and functions of Omnissa Workspace ONE® Hub Services
- Outline account options and permissions

4. Enterprise Integrations

- Outline the process and needs to integrate with directory services
- Explain certificate authentication and practical implementation with Workspace ONE
- Explain the benefits of integrating an email SMTP service into the Workspace ONE UEM console
- Describe Omnissa Dynamic Environment Manager™ and its architecture

5. Onboarding

- Outline the prerequisite configurations in the Workspace ONE UEM environment for onboarding devices for management
- Outline the steps for setting up autodiscovery in the Workspace ONE UEM console
- Enroll an endpoint through the Omnissa Workspace ONE® Intelligent Hub app
- Summarize platform onboarding options

6. Managing Endpoints

- Explain the differences between device and user profiles
- Describe policy management options for Windows and macOS
- Describe the functions and benefits of using compliance policies
- Explain the use cases for Freestyle Orchestrator
- Describe the capabilities that sensor and scripts enable.

7. Alternative Management Methods

- Describe the function and benefits of device staging
- Configure product provisioning in the Workspace ONE UEM console
- Understand the benefits of deploying a Omnissa Workspace ONE® Launcher™ configuration to Android devices

- List the system and device requirements for Linux device management in Workspace ONE UEM

8. Applications

- Describe the features, benefits, and capabilities of application management in Workspace ONE UEM

- Understand and configure deployment settings for public, internal, and paid applications in the Workspace ONE UEM console
- Describe the benefits of using Apple Business Manager content integration
- Describe the benefits of using server-to-client software distribution
- List the functions and benefits of Omnissa Workspace ONE® SDK

9. Device Email

- List the email clients supported by Workspace ONE UEM
- Configure an Exchange Active Sync profile in the Workspace ONE UEM console
- Configure Omnissa Workspace ONE® Boxer settings
- Summarize the available email infrastructure integration models and describe their workflows
- Configure email compliance policies and notifications services

10. Content Sharing

- Describe the benefits of using Content Gateway and the Content Gateway workflows
- Describe the benefits of integrating content repositories with Workspace ONE UEM
- Configure a repository in the Workspace ONE UEM console

11. Maintenance

- Manage endpoints from the Device List View and the Device Details View pages
- Analyze endpoint deployment and compliance data from Monitor Overview page

12. Omnissa Access

- Summarize the benefits of Omnissa Access
- Outline the core features and functions enabled by Omnissa Access
- Navigate the Omnissa Access console
- Explain the functions of directory integration with Omnissa Access
- Explain the various types of authentication protocols enabled by Omnissa Access

13. Integrating Workspace ONE UEM and Workspace ONE Access

- Explain the rationale for integrating Workspace ONE UEM and Omnissa Access
- Outline the process of connecting Workspace ONE UEM and Omnissa Access
- Examine the workflow of integrations
- Summarize the key features of an integrated solution

14. Productivity Integrations

- Identify the functions enabled by Omnissa Unified Access Gateway™
- Outline the purpose of the Workspace ONE UEM® Secure Email Gateway™ edge service
- Explain the features enabled by the Omnissa Omnissa Workspace ONE® Tunnel edge service
- Summarize the capabilities enabled by the Content Gateway edge service

15. SAML 2.0 Authentication

Workspace ONE Deploy & Manage

- Outline authentication methods supported by Omnissa Access
- Summarize the main properties of the SAML protocol
- Summarize the SAML authentication workflow
- Explain the application single sign-on authentication workflow with SAML

16. Mobile Single Sign-On

- Describe the concept of mobile single sign-on
- Outline mobile single sign-on workflows

17. Intelligence and Automation

- Summarize the features of Omnissa Workspace ONE Intelligence™
- Outline the benefits of using Workspace ONE Intelligence

