VMware Workspace ONE: Deploy and Manage [v22.x]

Course Duration: 40 Hours (5 Days)

Overview

The VMware Workspace ONE: Deploy and Manage [V22.x] course is a comprehensive training program designed to equip learners with the knowledge and skills necessary to implement and manage the Workspace ONE platform. This course covers the platform's architecture, administration, Enterprise integrations, Device onboarding, Endpoint management, Application deployment, Email configuration, Content sharing, and Maintenance. Participants will explore various aspects of the Workspace ONE solution, including how to navigate and customize the console, manage users and devices, configure Enterprise integrations, and ensure High availability. The course also delves into Productivity integrations, SAML 2.0 authentication, Mobile single sign-on, and the intelligence and automation features of Workspace ONE Intelligence. By the end of the course, learners will be well-versed in the Workspace ONE Deploy and Manage process, enabling them to efficiently deploy, manage, and secure devices and applications across an enterprise environment. This training is essential for IT professionals looking to harness the power of VMware's digital workspace platform to enhance organizational efficiency and security.

Audience Profile

The VMware Workspace ONE: Deploy and Manage [V22.x] course is designed for IT professionals seeking to master unified endpoint management.

- IT Administrators responsible for endpoint management and security
- Systems Engineers focused on enterprise mobility and digital workspace solutions
- Network Operations personnel involved in device management and security
- IT Security Professionals overseeing organizational device compliance and data protection
- Workspace ONE Solution Architects designing and implementing UEM strategies
- Support Technicians providing tier I/II support for managed devices
- Cloud Services Administrators managing SaaS solutions like Workspace ONE
- Systems Integrators deploying and managing cross-platform device management solutions
- IT Managers overseeing IT infrastructure and end-user computing environments
- Technical Consultants advising organizations on digital workspace solutions
- Mobility Specialists focusing on mobile device management and security
- Virtualization Specialists managing virtual desktops and applications
- Identity and Access Management Professionals working with SSO and authentication services
- Enterprise Architects planning IT frameworks that integrate with Workspace ONE
- Professionals aiming for VMware certifications related to Workspace ONE UEM
- IT Decision Makers evaluating or improving their organization's device management strategy

- Technical Sales Engineers and Pre-sales Analysts specializing in selling VMware solutions

Course Syllabus

Course Introduction

- Introductions and course logistics
- Course objectives

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

Administration

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

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 VMware Dynamic Environment Manager™ and its architecture

Onboarding

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

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.

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 VMware
- Workspace ONE® Launcher™ configuration to Android devices
- List the system and device requirements for Linux device management in Workspace ONE UEM

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 VMware Workspace ONE® SDK

Device Email

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

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

Maintenance

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

Workspace ONE Access

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

Integrating Workspace ONE UEM and Workspace ONE Access

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

Productivity Integrations

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

SAML 2.0 Authentication

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

Mobile Single Sign-On

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

Intelligence and Automation

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