TRAINOCATE

vmware LEARNING

VMware Workspace ONE: Skills for UEM plus Modern Management for Windows 10

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 and a modern Windows 10 management solution with VMware Workspace ONE®. Through a combination of hands-on labs, simulations, and interactive lectures, you will configure and manage the endpoint life cycle. You will investigate various methods for onboarding, securing, enabling, and maintaining Windows 10 with Workspace ONE. After the five days, you will have the foundational knowledge for effectively implementing VMware Workspace ONE® UEM and establishing the foundation of a modern management strategy.

Course Objectives

By the end of the course, you should be able to meet the following objectives:

- Explain the general features and functionality enabled with Workspace ONE UEM
- Summarize essential Workspace ONE administrative functions
- Summarize and implement common Workspace ONE integrations
- Explain the integration of Workspace ONE UEM with directory services
- Explain and deploy Workspace ONE edge services
- Onboard device endpoints into Workspace ONE UEM
- Securely deploy configurations to UEM managed devices
- Maintain environment and device fleet health
- Deploy applications to UEM managed devices
- Analyze a Workspace ONE UEM deployment
- Identify the Windows 10 management capabilities provided by the Workspace ONE solution to resolve traditional Windows management challenges
- Evaluate onboarding methodologies for Windows 10 devices
- Improve Windows 10 device security and the patch management experience by using the Workspace ONE security capabilities, including Profiles, Compliance, Baselines, Scripts, and Sensors
- Distribute Windows 10 software, including Windows Store for Business and native Windows applications, to enrolled Windows 10 devices to streamline access to business-critical Windows software
- Implement intelligence-driven vulnerability monitoring and identify actionable steps to resolve issues

Target Audience

- VMware Workspace ONE® UEM operators and administrators, account managers, solutions architects, solutions engineers, sales engineers, and consultants
- Legacy Windows management administrators with the requisite knowledge of Workspace ONE UEM

vmware PARTNER
AUTHORIZED TRAINING RESELLER

Prerequisites

This course has no prerequisites.

Course Delivery Options

- Classroom
- Live Online
- Private Training

Product Alignment

- VMware Workspace ONE UEM
- VMware Workspace ONE® Intelligence™
- VMware Workspace ONE® Access™
- VMware Carbon Black

vmware PARTNER
AUTHORIZED TRAINING RESELLER

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

3 Administration
- Explain the features and functions of Workspace ONE Hub Services
- Summarize hierarchical management structure
- Navigate and customize the Workspace ONE UEM console
- 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

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 via the 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 10 and macOS

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 Workspace ONE Launcher configuration to Android devices

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 the Workspace ONE Software Development Kit (SDK)

9 Device Email
- Outline email clients supported by Workspace ONE UEM
- Configure an Exchange Active Sync (EAS) profile in the Workspace ONE UEM console
- Configure Workspace ONE® Boxer settings
- Summarize the available email infrastructure integration models and describe their workflows

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
- Identify console tools that support maintenance
- Analyze how to implement compliance policies to protect environmental security

- Outline features and functions enabled by Workspace ONE Assist

12 Intelligence and Automation

- Outline the functionality enabled by Workspace ONE Intelligence
- Summarize and deploy automation
- Describe the functions and benefits of using compliance policies
- Explain the use-case for Freestyle Orchestrator and understand Freestyle Workflows
- Outline the capabilities of sensors and scripts and the steps for creating them

13 Windows Management

- Identify the key challenges of traditional Windows management solutions in device management, security, and user enablement
- Outline the device management capabilities provided by Workspace ONE that resolve Windows 10 device management challenges with Windows Security Management
- Summarize the security management capabilities provided by Workspace ONE that address Windows 10 security management challenges
- Describe how the Workspace ONE solution enables the unified catalog and self-service capabilities to improve the end-user experience

14 Device Onboarding

- Describe the benefits of onboarding Windows 10 endpoints to Workspace ONE
- Onboard Windows 10 devices using the agent-based enrollment method
- Onboard Windows 10 devices using command line enrollment
- Onboard Windows 10 devices using one of the Microsoft Azure AD enrollment options
- Onboard Windows 10 devices using the factory provisioning experience
- Onboard Windows 10 devices using VMware ONE® AirLift™

15 Device Security

- Outline the capabilities in Workspace ONE UEM that improve Windows 10 device security
- Deploy profiles to Windows 10 devices to enforce corporate security requirements
- Deploy baselines to Windows 10 devices to ensure that they are compliant with defined Windows 10 security benchmarks
- Construct a modern Windows 10 update and patch management strategy based upon your business requirements
- Deploy sensors to Windows 10 devices to collect custom metrics
- Deploy scripts to Windows 10 devices to execute customized commands
- List the additional Windows 10 security management benefits provided by VMware Carbon Black

16 Software Distribution

- Outline the software distribution and management capabilities provided by Workspace ONE UEM
- Integrate Microsoft Store for Business with Workspace ONE UEM and distribute Microsoft Store for Business applications to Windows 10 devices
- Articulate the importance of establishing a content distribution network for Windows software distribution and configure Peer Distribution
- Manage existing Windows applications and software in your Workspace ONE UEM console based upon your unique business requirements, including managing application updates, transformations, and assignments
- Migrate existing Windows software packages from Configuration Manager to Workspace ONE UEM

17 Administration and Maintenance

- Implement Workspace ONE Intelligence to monitor Windows 10 devices
- Construct a CVE Device Health Comparison Report and interpret its findings.
- Interpret Risk Score assessments to formulate a resolution plan

Contact

If you have questions or need help registering for this course, click here.