

Workspace ONE: Configure and manage

Course Duration: 40 Hours/ 5 days

Course objectives

- Understand the course scope, structure, and role-based outcomes for Workspace ONE configuration and management.
- Describe the Workspace ONE platform, architecture, and core services.
- Navigate and configure core settings in the Workspace ONE UEM Console.
- Manage users, groups, and organizational structures in Workspace ONE UEM.
- Integrate Workspace ONE UEM with key enterprise services and systems.
- Configure and manage secure device enrollment methods.
- Create and enforce device compliance and management policies.
- Monitor and manage devices throughout their lifecycle.
- Deploy and manage applications across supported platforms.
- Configure secure mobile email and content access.
- Provide remote support and troubleshooting for managed devices.
- Apply Workspace ONE security features to protect devices and data.
- Configure secure access and authentication using Omnisia Access.
- Automate administrative tasks using Workspace ONE workflows.
- Use analytics and reports to monitor environment health.

Target audience

- Intermediate to advanced practitioners that design, deploy, manage, optimize, troubleshoot, and secure the Digital Workspace.

Prerequisites Recommended:

- Understand fundamental Networking / Storage and Infrastructure concepts
- A working knowledge of Workspace ONE
- Automate administrative tasks using Workspace ONE workflows.
- Use analytics and reports to monitor environment health.
- A background in End-User Computing

Course modules

Mod-1 Course introduction

- Introductions and course logistics
- Course objectives

Mod- 2 Understanding Workspace ONE

- What is Workspace ONE?
- Workspace ONE components and architecture
- Workspace ONE Intelligent Hub & Hub Services

Mod-3 Console navigation and settings

- Navigating the Workspace ONE UEM console
- Configuring system settings and customization

Mod- 4 User and group management

- User types and roles

- Organization groups
- Groups

Mod- 5 Enterprise integrations

- Directory Services and ACC
- Certificate Authorities
- Dynamic Environment Manager
- Additional integrations
- Network considerations

Mod- 6 Device enrollment

- Device enrollment overview
- Intelligent Hub enrollment
- Windows Desktop and Server enrollment
- Windows Multiuser
- Automated Device Enrollment for Apple devices
- Linux web enrollment
- Enrolling Google Endpoints

Mod- 7 Policies

- Introduction to profiles and baselines
- Profiles
- Baselines
- Compliance policies

Mod- 8 Device Management

- Device Details walkthrough
- Critical device actions
- Scripts, sensors, and tags
- Platform updates

Mod- 9 Applications

- Applications Overview
- Public Applications
- Internal Applications
- Purchased Applications
- App Volume Integrations

Mod- 10 Mobile email and content management

- Deploying Managed Email Settings
- PowerShell Integration
- Workspace ONE Secure Email Gateway
- Gmail integration
- Email compliance and Email Notification Service
- Content management

Mod- 11 Remote support

- Workspace ONE Assist
- Workspace ONE ITSM Connector
- Intel vPro® integration
- Remote log collection and troubleshooting

Mod- 12 Security

- Zero trust

- Identity and authentication
- Vulnerability Defense
- Mobile Threat Defense
- Workspace ONE Tunnel
- Security integrations

Mod- 13 Omnissa Access

- Introduction to Omnissa Access
- User management
- App/resource catalog
- Authentication and policies
- Reporting and logs

Mod- 14 Automating workflows

- Freestyle Orchestrator
- Creating workflows in Workspace ONE UEM
- Creating workflows in Omnissa Intelligence
- Workspace ONE APIs

Mod- 15 Analytics and reporting

- Dashboards and reporting in UEM
- Omnissa Intelligence
- Experience Management