Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

**Sie erreichen uns hier**

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com
Phone: +43 1 370 94 40 - 34

# MD-102T00 : Microsoft 365 Endpoint Administrator

| CODE: | LÄNGE: | PREIS: |
|---|---|---|
| MCS_MD-102T00A | 40 Hours (5 Tage) | €2,590.00 |

## Description

In diesem Training lernen die Teilnehmenden, wie sie eine Endpunktbereitstellungsstrategie mithilfe moderner Bereitstellungsverfahren und der Anwendung von Updatestrategien planen und umsetzen.
Der Training behandelt wesentliche Elemente der modernen Verwaltung, Co-Management-Ansätze und die Microsoft Intune-Integration. Die App-Bereitstellung, die Verwaltung browserbasierter Anwendungen und wichtige Sicherheitskonzepte wie Authentifizierung, Identitäten, Zugriff und Compliancerichtlinien werden erläutert. Technologien wie Microsoft Entra ID, Azure Information Protection und Microsoft Defender for Endpoint werden erkundet, um Geräte und Daten zu schützen.

## Zielgruppe

Microsoft 365-Endpunktadministrator*innen sind für die Bereitstellung, Konfiguration, den Schutz, die Verwaltung und die Überwachung von Geräten und Clientanwendungen in Unternehmen zuständig. Zu ihren Aufgaben gehört die Verwaltung von Identitäten, Zugriff, Richtlinien, Updates und Anwendungen.
Sie arbeiten mit Microsoft 365 Enterprise-Administrator*innen zusammen, um eine Gerätestrategie zu entwickeln und umzusetzen, die den Anforderungen einer modernen Organisation entspricht. Microsoft 365-Endpunktadministrator*innen sollten sich mit Microsoft 365-Workloads auskennen und über umfassende Kenntnisse und Erfahrungen in der Bereitstellung, Konfiguration und Wartung von Windows 11 und höher sowie Geräten mit anderen Betriebssystemen als Windows verfügen. Bei dieser Rolle liegt der Schwerpunkt auf Clouddiensten statt auf lokalen Verwaltungstechnologien.

## Voraussetzungen

Windows Grundlagen für Administratoren
oder
Windows Client Fundamentals

## Inhalt

Examine benefits of modern management
Examine the enterprise desktop life-cycle model
Examine planning and purchasing
Examine desktop deployment
Plan an application deployment
Explore the Enterprise Desktop — Plan for upgrades and retirement — Explore Windows Editions
Examine Windows client editions and capabilities
Select client edition
Examine hardware requirements — Understand Microsoft Entra ID
Examine Microsoft Entra ID
Compare Microsoft Entra ID and Active Directory Domain Services
Examine Microsoft Entra ID as a directory service for cloud apps
Compare Microsoft Entra ID P1 and P2 plans
Examine Microsoft Entra Domain Services — Manage Microsoft Entra identities
Examine RBAC and user roles in Microsoft Entra ID
Create and manage users in Microsoft Entra ID
Create and manage groups in Microsoft Entra ID
Manage Microsoft Entra objects with PowerShell
Synchronize objects from AD DS to Microsoft Entra ID — Manage device authentication

Describe Microsoft Entra join
Examine Microsoft Entra join prerequisites limitations and benefits
Join devices to Microsoft Entra ID
Manage devices joined to Microsoft Entra ID
Enroll devices using Microsoft Configuration Manager
Deploy the Microsoft Configuration Manager client
Monitor the Microsoft Configuration Manager client
Manage the Microsoft Configuration Manager client
Enroll devices using Microsoft Intune
Manage mobile devices with Intune
Enable mobile device management
Explain considerations for device enrollment
Manage corporate enrollment policy
Enroll Windows devices in Intune
Enroll Android devices in Intune
Enroll iOS devices in Intune
Explore device enrollment manager
Explore Intune device profiles
Monitor device enrollment
Create device profiles
Manage devices remotely
Create a custom device profile
Knowledge check
Execute device profiles
Knowledge check
Oversee device profiles
Examine user profile
Explore user profile types
Examine options for minimizing user profile size
Monitor device profiles in Intune
Deploy and configure folder redirection
Manage device sync in Intune
Sync user state with Enterprise State Roaming
Manage devices in Intune using scripts
Maintain user profiles
Configure Enterprise State Roaming in Azure
Examine mobile application management
Examine considerations for mobile application management
Prepare line-of-business apps for app protection policies
Implement mobile application management policies in Intune
Execute mobile application management
Manage mobile application management policies in Intune
Deploy applications with Intune
Add apps to Intune
Manage Win32 apps with Intune
Deploy applications with Configuration Manager
Deploying applications with Group Policy
Assign and publish software
Explore Microsoft Store for Business
Implement Microsoft Store Apps
Update Microsoft Store Apps with Intune
Deploy and update applications
Assign apps to company employees
Administer endpoint applications
Manage apps with Intune
Manage Apps on non-enrolled devices
Deploy Microsoft 365 Apps with Intune
Additional Microsoft 365 Apps Deployment Tools
Configure Microsoft Edge Internet Explorer mode
App Inventory Review
Protect identities in Microsoft Entra ID
Explore Windows Hello for Business
Deploy Windows Hello
Manage Windows Hello for Business
Explore Microsoft Entra ID Protection
Manage self-service password reset in Microsoft Entra ID
Implement multi-factor authentication
Enable organizational access
Protect access to resources using Intune
Enable access to organization resources
Explore device compliance policy
Explore VPN types and configuration
Deploy a device compliance policy
Explore Always On VPN
Explore conditional access
Deploy Always On VPN
Implement device compliance
Create conditional access policies
Report enrolled devices inventory in Intune
Monitor and report device compliance
Build custom Intune inventory reports
Generate inventory and compliance reports
Access Intune using Microsoft Graph API
Deploy device data protection
Explore Windows Information Protection
Plan Windows Information Protection
Implement and use Windows Information Protection
Explore Encrypting File System in Windows client
Explore BitLocker
Manage Microsoft Defender for Endpoint

Explore Microsoft Defender for Endpoint
Examine key capabilities of Microsoft Defender for Endpoint
Explore Windows Defender Application Control and Device Guard
Explore Microsoft Defender Application Guard
Examine Windows Defender Exploit Guard
Explore Windows Defender System Guard
Explore Windows Security Center
Explore Windows Defender Credential Guard
Manage Microsoft Defender Antivirus
Manage Windows Defender Firewall
Explore Windows Defender Firewall with Advanced Security
Explore Microsoft Defender for Cloud Apps
Planning Microsoft Defender for Cloud Apps
Implement Microsoft Defender for Cloud Apps
Assess deployment readiness
Examine deployment guidelines
Explore readiness tools
Assess application compatibility
Explore tools for application compatibility mitigation
Prepare network and directory for deployment
Plan a pilot
Evaluate traditional deployment methods
Set up the Microsoft Deployment Toolkit for client deployment
Manage and deploy images using the Microsoft Deployment Toolkit
Explore client deployment using Configuration Manager
Examine deployment components of Configuration Manager
Manage client deployment using Configuration Manager
Plan in-place upgrades using Configuration Manager
Use Autopilot for modern deployment
Examine requirements for Windows Autopilot
Prepare device IDs for Autopilot
Implement device registration and out-of-the-box customization
Examine Autopilot scenarios
Troubleshoot Windows Autopilot
Examine subscription activation
Deploy using provisioning packages
Use Windows Configuration Designer
Use Microsoft Entra join with automatic MDM enrollment
Explore using co-management to transition to modern endpoint management
Examine prerequisites for co-management
Evaluate modern management considerations
Evaluate upgrades and migrations in modern transitioning
Migrate data when modern transitioning
Migrate workloads when modern transitioning
Examine Azure Virtual Desktop
Explore Azure Virtual Desktop
Configure Azure Virtual Desktop
Administer Azure Virtual Desktop

Manage Microsoft Defender in Windows client

Deploy using the Microsoft Deployment Toolkit

Deploy using Microsoft Configuration Manager

Deploy Devices using Windows Autopilot

Implement dynamic deployment methods

Plan a transition to modern endpoint management

Explore Windows 365
Configure Windows 365
Manage Windows 365
Administer Windows 365

Manage Azure Virtual Desktop

## Test und Zertifizierung

Wichtige Information
Dieses Training behandelt prüfungsrelevante Themen zum Microsoft Examen: MD-102 Endpoint Administrator
HINWEIS:
Um während des Trainings an den Übungen teilnehmen zu können, ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich. Dafür benötigen Sie ein Mobiltelefon und eine Authentifizierungs-App. Wir empfehlen die kostenlose Microsoft Mobile Phone Authenticator App.
Download Microsoft Mobile Phone Authenticator App.
Set up your Microsoft 365 sign-in for multi-factor authentication.

## Kurstermine

| Datum | Lokation | Time Zone | Sprache | Type | Durchführungsgarantie | PREIS |
|---|---|---|---|---|---|---|
| 18 Aug 2025 | Wien | CEDT | German | Classroom | | €2,590.00 |
| 18 Aug 2025 | Wien | CEDT | German | Instructor Led Online | | €2,590.00 |
| 25 Aug 2025 | Wien | CEDT | German | Classroom | | €2,590.00 |
| 25 Aug 2025 | Wien | CEDT | German | Instructor Led Online | | €2,590.00 |

## Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.