Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Microsoft 365 Modern Desktop Administrator Fast Track

CODE:	LENGTH:	PRICE:
MCS_FTMD-1001X	40 Hours (5 days)	kr36,000.00

Description

The Microsoft 365 Modern Desktop Administrator Associate – Fast Track bundles the courses:
MD-100 Windows Client
MD-101: Managing Modern Desktops
You will learn to support and configure Windows 10 desktops in a corporate environment. You will acquire the necessary knowledge for installing, customizing and updating Windows 10 operating systems. You'll also learn how to manage storage, files, and devices, as well as configure network connectivity for Windows 10. Other topics include securing Windows 10, protecting data on devices and troubleshooting Windows
You will also learn to plan and implement an operating system deployment and update strategy. Learn the key components of modern management and co-management strategies and how to integrate Microsoft Intune into your business. You will also learn methods for deploying and managing apps and browser-based applications.
Another topic is key concepts of security in modern administration such as authentication, identities, access and compliance policies. Participants will learn about Azure Active Directory, Azure Information Protection, and Windows Defender Advanced Threat Protection and how to use them to protect devices and data.

Objectives

Installing and customizing Windows clients
Configure updates for Windows
Configure devices and drivers for Windows Configure storage for Windows
Configure network and remote management settings in Windows
Configure and manage browsers and applications on Windows
Configure account access and authentication
Configure file and folder permissions
Describe methods for protecting Windows clients, common threats, and risk mitigation methods.
Troubleshoot Windows and application installation problems
Troubleshoot hardware and driver issues
Troubleshoot file issues and perform restores
Planning, developing and establishing an operating system deployment, upgrade and upgrade strategy.
Understand the benefits and methods of co-management strategies.
Planning and setting up device registration and configuration.
Manage and deploy applications and plan a mobile application management strategy.
Manage users and authenticate with Azure AD and Active Directory DS.
Describe and establish methods to protect devices and data.

Audience

The Modern Desktop Administrator distributes, configures, secures, manages, and monitors devices and client applications in an enterprise environment. MDA’s responsibilities include managing identity, access, policies, updates, and applications. The MDA works with the M365 Enterprise Administrator to develop and implement a device strategy that meets the business needs of a modern enterprise. The Modern Desktop Administrator must be familiar with M365 workloads and have extensive skills and experience in deploying, configuring, and maintaining Windows 10+ and non-Windows devices. The MDA's role focuses on cloud services rather than on-premises management technologies.

Prerequisites

Basic knowledge of computer networks and hardware concepts
A basic understanding of operating system and application concepts

Experience using the Windows operating system
The Modern Desktop Administrator must be familiar with M365 workloads and have extensive skills and experience in deploying, configuring, and maintaining Windows 10+ and non-Windows devices. The MDA's role focuses on cloud services rather than on-premises management technologies.

Programme

Module 1: Installing Windows
This module covers installing the Windows 10 OS. Students will learn the different editions of Windows 10, requirements, and new features introduced. This module covers how to install the OS, as well as methods for migrations and upgrading. Students will also learn about common tools used in the deployment process.
Lessons:
• Introducing Windows 10
• Windows 10 Editions and Requirements
• Deployment Options
• Upgrading to Windows 10
• Deployment Tools
After completing this module, students will be able to:
• Understanding the different editions and features of Windows 10.
• Understand the Windows 10 client installation options.
• Practice installing Windows 10.
• Migrate content using the User State Migration Tool.
Module 2: Post-installation Configuration and Personalization
This module covers common post-installation tasks in Windows 10. Students will learn how to customize the user interface, as well as using the control panel and settings app to configure common OS settings. This course will also introduce students to Windows PowerShell. This module will cover how device drivers work and how they work. Students will also be introduced to managing and configuring hardware peripherals such as printers.
Lessons:
• Configure and Customize the Windows Start Menu
• Common Configuration Options
• Advanced Configuration Methods
• Managing Drivers and Devices
After completing this module, students will be able to:
• Customize the Windows 10 UI
• Configure device specific settings such as power plans and mobile device options.
• Use the Windows control panel and setting app to configure settings.
• Perform tasks using Windows PowerShell.
• Describe concepts related to drivers.
• Describe printer management concepts.
• Configure client
-side printing and managing print server properties.
Module 3: Updating Windows in Windows 10
In this module, Students will learn about keeping Windows 10 up-to-date. Students will be introduced to the new Windows servicing model and how it applies to various scenarios.
Students will learn the various different methods for updating Windows and applications, as well as managing updates using tools like group policy and Windows Update for Business.
Lessons:
• Windows Servicing Model
• Updating Windows
•
After completing this module, students will be able to:
• Describe the Windows servicing model.
• Configure Windows update settings.
• Describe updating Windows using WSUS.
• Describe updating Windows using Windows Update for Business.
• Configure Windows update using group policy.
Module 4: Configuring Networking
In this module, Students will learn about networking concepts. This module will introduce to IPv4 and IPv6, and concepts like DNS. Students will learn how to configure network settings in Windows, as well as learn about wireless network technologies. The module will conclude with methods of managing Windows remotely.
Lessons:
• Configure IP Network Connectivity
• Implement Name Resolution
• Implement Wireless Network Connectivity
• Remote Access Overview
• Remote Management
•
After completing this module, students will be able to:

• Configure IP network connectivity.
• Describe how name resolution works.
• Describe remote access technologies like VPNs.
• Configure Windows for remote management and access.

Module 5: Configuring Storage

This module covers storage configuration and management in Windows 10. Students will be introduced to local, cloud and virtual storage options. This course will also cover configuring storage on client devices and introduce storage spaces.

Lessons:

• Overview of storage options
• Managing Local Storage
• Maintaining Disks and Volumes
• Managing Storage Spaces
• Describe the options and benefits of local, cloud, and virtual storage.
• Configure OneDrive.
• Configure local disk partitions and volumes.
• Describe the capabilities and benefits of Storage spaces.

Module 6: Managing Apps in Windows 10

In this module, Students will be introduced to App management in Windows 10. This module will cover the different types of apps and supported installation methods. Students will learn how to install apps using manual and automated methods, as well as manage app delivery using the Windows Store. Finally, this module will cover the differences between Internet Explorer and Microsoft Edge.

Lessons:

• Providing Apps to Users
• Managing Universal Windows Apps
• Web Browsers in Windows 10

After completing this module, students will be able to:

• Describe the different types of applications.
• Install applications manually and using automated methods.
• Manage application deployment using the Windows Store.
• Learn about web browser features in Windows 10.

Module 7: Configuring Authorization & Authentication

This module introduces the tools and features of Windows 10 for authorizing access to Windows 10 clients. Students will learn about methods for how users sign-in to Windows 10. This module also covers restricting what users can or cannot do on a device through methods like UAC and account types.

Lessons:

• Authentication
• Configuring User Account Control
• Implementing Device Registration

After completing this module, students will be able to:

• Describe the different methods for securing data and the Windows 10 OS.
• Describe the different types of user and service accounts.
• Configure Windows Hello.
• Configure user account control.

Module 8: Configuring Data Access and Usage

In this module, Students will learn about permissions. This module will cover considerations for different files systems. Students will learn how to configure file and folder permissions as well
as shared folders. The module will conclude with configuring settings through methods such as local and group policy.

Lessons:

• Overview of File Systems
• Configuring and Managing File Access
• Configuring and Managing Shared Folders

After completing this module, students will be able to:

• Describe the differences and benefits of supported file systems.
• Configure file and folder permissions.
• Configure shared folders.
• Secure Windows through local policy settings.

Module 9: Configuring Threat Protection and Advanced Security

This module introduces students to protecting devices from external threats. Students will learn about the different types of common threats. This module will teach students about using encryption, firewalls, and IPSec to help protect against threats. The module will conclude with how to configure and use Windows Defender and AppLocker.

Lessons:

• Malware and Threat Protection
• Windows Defender
• Connection Security Rules
• Advanced Protection Methods

After completing this module, students will be able to:

• Identify common security threats .
• Describe the methods by which you can mitigate these common security threats.
• Describe the different methods of encryption.

• Describe how Windows firewall can secure the device.
• Describe the benefits of using IPSec.
• Describe the different features of Windows Defender.
• Describe the benefits of using AppLocker.

Module 10: Supporting the Windows 10 Environment

This module will cover the Windows 10 architecture and common environments. Students will be introduced to the various tools used in maintaining Windows. This module will also discuss methodologies for effectively troubleshooting issues and how to proactively manage and optimize Windows 10.

Lessons:
• Windows Architecture
• Support and Diagnostic Tools
• Monitoring and Troubleshooting Computer Performance

After completing this module, students will be able to:
• Describe the Windows architecture.
• Describe key stages in troubleshooting.
• Describe the purpose and benefits of the various tools in Windows.
• Use monitoring tools to establish a performance baseline
• Optimize performance on Windows 10 clients.

Module 11: Troubleshooting Files & Applications

This module helps students plan for file backup and recovery. Students will learn how to plan and configure data protection strategies and how to perform various file and system recovery methods. This module also includes common methods for troubleshooting application installation issues, compatibility issues, and resolving browser issues.

Lessons:
• File Recovery in Windows 10
• Application Troubleshooting

After completing this module, students will be able to:
• Describe the different methods of file recovery.
• Configure Windows 10 to support individual file and system recovery.
• Recover a device using the Reset This PC function.
• Solve application compatibility issues with the Application Compatibility Toolkit.
• Troubleshoot common browser issues.

Module 12: Troubleshooting the OS

In this module, Students will learn how to troubleshoot startup and service issues related to the operating system. This module will teach the different startup and recovery options, and how to troubleshoot different Windows services.

Lessons:
• Troubleshooting Windows Startup
• Troubleshooting Operating System Service Issues

After completing this module, students will be able to:
• Describe the various methods identifying and recovering from startup issues.
• Describe when to use the various advanced startup options.
• Identify and disable a failed service.
• Identify and mitigate common locked account scenarios.

Module 13: Troubleshooting Hardware and Drivers

This module introduces hardware troubleshooting. Students will learn about driver management and how to troubleshoot devices. Students will also learn steps for troubleshooting system hardware and external peripherals such as USB drives and printers, including diagnostic methods and remediation.

Lessons:
• Troubleshooting Device Driver Failures
• Overview of Hardware Troubleshooting
• Troubleshooting Physical Failures

After completing this module, students will be able to:
• Troubleshoot and remediate driver issues.
• Troubleshoot Peripherals
• Diagnose and replace hardware.

Module 14: Planning an Operating System Deployment Strategy

This module explains how to plan and implement a deployment strategy. Students will learn about the concepts of supporting the desktop through it's entire lifecycle. This module also covers assessing an existing environment and the tools used to prepare a deployment strategy. Finally, students will be introduced to the tools and strategies used for desktop deployment.

Lessons:
• The Enterprise Desktop
• Assessing Deployment Readiness
• Deployment Tools & Strategies

After completing this module, students will be able to:
• Describe the enterprise desktop lifecycle.
• Describe how to assess an existing environment
• Describe methods for mitigating deployment blockers.
• Describe the different tools and methods for deployment.

Module 15: Implementing Windows 10

This module covers the modern methods of Windows deployment used in common scenarios such as upgrading and migrating to

Windows 10, as well as deploying new devices and refreshing existing devices. Students will also learn about alternate methods of OS deployment as well as considerations when choosing methods of deployment.
Lessons:
• Upgrading Devices to Windows 10
• Deploying New Devices and Refreshing
• Migrating Devices to Windows 10
• Alternate Deployment Methods
• Imaging Considerations
• Creating and deploying provisioning package
• Migrating user settings
• Deploying Windows 10 with AutoPilot
After completing this course, learners should be able to:
• Develop an Operating System deployment and upgrade strategy
• Understand the different methods of deployment.
• Understand which scenarios on
-premise and cloud-based solutions can be used for.
• Deploy and migrate desktops to Windows 10.
Module 16: Managing Updates for Windows 10
This module covers managing updates to Windows. This module introduces the servicing options for Windows 10. Students will learn the different methods for deploying updates and how to configure windows update policies. Finally, students will learn how to ensure and monitor update compliance using Windows Analytics.
Lessons:
• Updating Windows 10
• Windows Update for Business
• Introduction to Windows Analytics
• Manually configuring Windows Update settings
• Configuring Windows Update by using GPOs
After completing this module, students will be able to:
• Describe the Windows 10 servicing channels.
• Configure a Windows update policy using Group Policy settings.
• Configure Windows Update for Business to deploy OS updates.
• Use Windows Analytics to assess upgrade readiness and update compliance.
Module 17: Device Enrollment
In this module, students will examine the benefits and prerequisites for co-management and learn how to plan for it. This module will also cover Azure AD join and will be introduced to Microsoft Intune, as well as learn how to configure policies for enrolling devices. The module will conclude with an overview of device inventory in Intune and reporting using the Intune console, Power BI and Microsoft Graph.
Lessons:
• Device management options
• Microsoft Intune Overview
• Manage Intune device enrollment and inventory
• Managing devices with Intune
After completing this module, students will be able to:
• Describe benefits and methods for migrating to co
-management.
• Deploy an MDM with Microsoft Intune.
• Configure device enrollment.
• Enroll desktop and mobile devices in Windows Intune.
• Configure and downloads inventory reports.
Module 18: Configuring Profiles
This module dives deeper into Intune device profiles including the types of device profiles and the difference between built-in and custom profiles. The student will learn about assigning profiles to Azure AD groups and monitoring devices and profiles in Intune. The module will conclude with an overview of using Windows Analytics for health and compliance reporting.
Lessons:
• Configuring device profiles
• Managing user profiles
• Monitoring devices
After completing this module, students will be able to:
• Describe the types of device profiles.
• Create and assign device profiles.
• Configure user profile and folder redirection.
• Monitor and report on devices using Intune and Windows Analytics.
Module 19: Application Management
In this module, students learn about application management on-premise and cloud-based solutions. This module will cover how to manage Office 365 ProPlus deployments in Intune as well as how to manage apps on non-enrolled devices. The module will conclude with an overview of Enterprise Mode with Internet Explorer and Microsoft Edge and tracking your installed applications, licenses, and assigned apps using Intune.
Lessons:
• Implement Mobile Application Management (MAM)

• Deploying and updating applications
• Administering applications
After completing this module, students will be able to:
• Describe the methods for application management.
• Deploy applications using Intune and Group Policy.
• Configure Microsoft Store for Business.
• Deploy Office365 ProPlus using Intune.
• Manage and report application inventory and licenses.
Module 20: Managing Authentication in Azure AD
In this module, students well be introduced to the concept of directory in the cloud with Azure AD. Students will learn the similarities and differences between Azure AD and Active Directory DS and how to synchronize between the two. Students will explore identity management in Azure AD and learn about identity protection using Windows Hello for Business, as well as Azure AD Identity Protection and multi-factor authentication.
Lessons:
• Azure AD Overview
• Managing identities in Azure AD
• Protecting identities in Azure AD
• Managing device authentication
After completing this module, students will be able to:
• Describe the capabilities of Azure AD.
• Manage users using Azure AD with Active Directory DS.
• Implement Windows Hello for Business.
• Join devices to Azure AD.
Module 21: Managing Device Access and Compliance
In this module, students will be introduced to managing device security. The module will cover securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10. Students will learn how to create and deploy compliance policies and use compliance policies for conditional access. The module concludes with monitoring devices enrolled in Intune.
Lessons:
• Microsoft Intune Overview
• Implement device compliance policies
After completing this module, students will be able to:
• Describe methods of enabling access from external networks.
• Deploy compliance and conditional access policies.
• Use Intune to monitor device compliance.
Module 22: Managing Security
In this module, students will learn about data protection. Topics will include Windows & Azure Information Protection, and various encryption technologies supported in Windows 10. This module also covers key capabilities of Windows Defender Advanced Threat Protection and how to implement these capabilities on devices in your organization. The module concludes using Windows Defender and using functionalities such as antivirus, firewall and Credential Guard.
Lessons:
• Implement device data protection
• Managing Windows Defender ATP
• Managing Windows Defender in Windows 10
After completing this module, students will be able to:
• Describe the methods protecting device data.
• Describe the capabilities and benefits of Windows ATP
• Deploy and manage settings for Windows Defender clients.

Test and Certification

Exam MD-100 and MD-101 for certification as Microsoft 365 Certified Modern Desktop Administrator Associate Training

Further Information

Lab Overview:
-In-place upgrade from Win7 to Win 10
-Migrating User Settings using USMT
-Using Settings App & Control PanelLab : Using Group Policy Objects
-Using PowerShell to Configure Windows
-Managing local and network printers
-Updating Windows 10
-Configuring Network Connectivity
-Configuring and Testing Name Resolution
-Remote management
-Managing StorageLab: Compressing Folders
-Enabling disk quotas

-Creating a Storage Space
-Synchronizing files with OneDrive
-Sideloading to app
-Installing and updating Microsoft Store apps
-Configuring Internet Explorer Enterprise Mode
-Joining a domain
-Creating Security Policies
-Configuring UAC
-Creating, Managing, and Sharing a Folder
-Using Conditions to Control Access and Effective Permissions
-Configuring Windows Defender
-Creating Firewall Rules
-Creating Connection Security Rules
-Using EFS
-Using Bitlocker
-Configuring AppLocker
-Configuring Windows Defender
-Creating Firewall Rules
-Creating Connection Security Rules
-Using EFS
-Using Bitlocker
-Configuring AppLocker
-Using File History to Recover Files
-Troubleshooting desktop apps
-Troubleshooting application compatibility issues
-Troubleshooting Microsoft Edge Issues
-Recovering using Reset This PC
-Recovering using a Restore Point
-Recovering using Driver Rollback
-Planning Windows 10 deployment
-Implementing Windows 1
-Managing Updates for Windows 10
-Device Enrollment and Management
-Managing profiles
-Managing Applications
-Managing objects and authentication in Azure AD
-Managing Access and Compliance
-Managing Security in Windows 10

Session Dates

På begäran, kontakta oss

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.