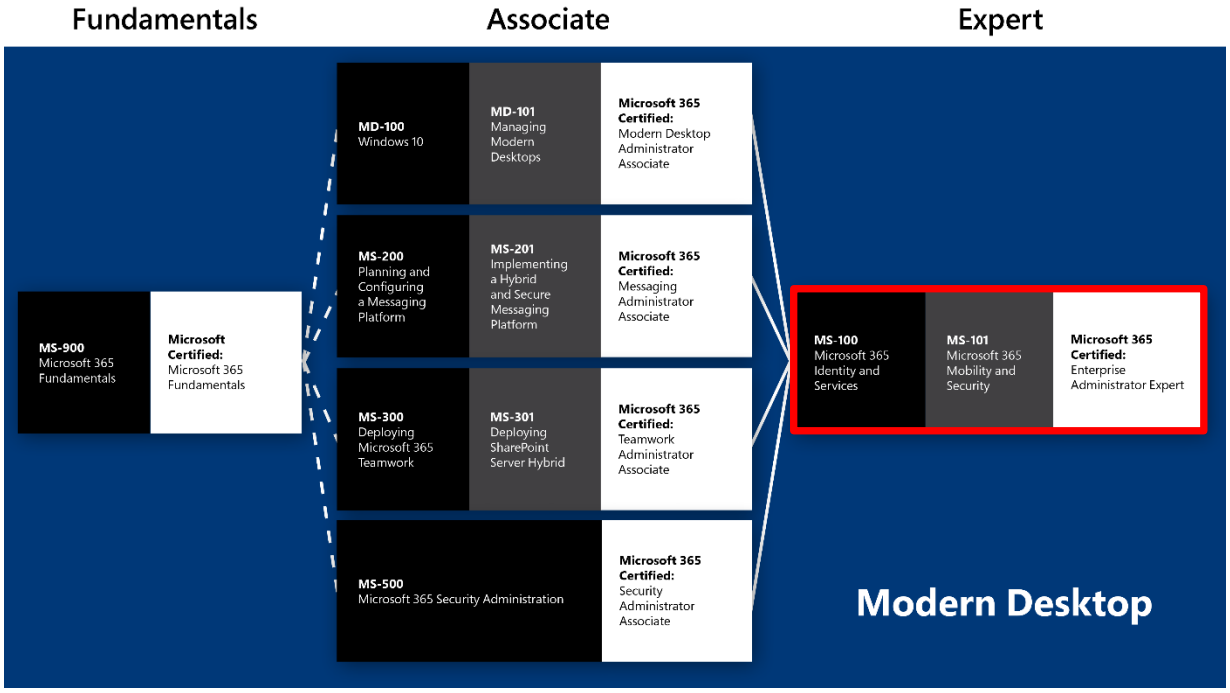
MS100-101 - Microsoft 365 Certified: Enterprise Administrator Expert

These 2 courses are designed for IT Professionals who will learn how to plan an Office 365 deployment, how to configure Office 365, and how to manage Office 365 ProPlus deployments.

These courses help prepare for the exams « MS-100 - Microsoft 365 Identity and Services » and « MS-101: Microsoft 365 Mobility and Security » to obtain the title « Microsoft 365 Certified: Enterprise Administrator Expert ».



1. MS-100 - Microsoft 365 Identity and Services

Overview

This course is divided into 3 complementary parts :

1.1. Office 365 Management

This course introduces you to the key components of Office 365 and then focuses on what it takes to move your organization to Office 365. You will spend time learning how to plan an Office 365 deployment, how to configure Office 365, and how to manage Office 365 ProPlus deployments. The course begins with an introduction to the core components of Office 365. You will begin by examining Exchange Online, including how to create and manage recipients, as well as how to manage anti-malware, anti-spam, and your disaster recovery needs. This is followed by an introduction to retention policies and tags, including how to plan for migration strategies and how to select the right migration option for your organization. You will also learn how to migrate mailboxes to Office 365 in a hybrid deployment.

The course then introduces you to SharePoint Online. You will learn how to create a SharePoint hybrid environment and how to manage your local site. This includes an introduction to the encryption services used by SharePoint Online, as well as data loss prevention and anti-malware protection. From SharePoint Online, you will transition to Microsoft Teams. You will examine how to use collaboration apps in Office 365, and you will be introduced to user authentication, guest access, audio conferencing, and implementing phone systems.

Following this introduction to Office 365 components, the course takes a deep dive into what it takes to move an organization to Office 365. Since every successful deployment is a product of extensive planning, this course focuses on how to plan for network requirements, service setup, and a hybrid environment. This includes planning for a hybrid Exchange environment, a hybrid SharePoint environment, and a hybrid Skype for Business environment. The course then examines what it takes to migrate your organization to Office 365, including how to clean up Active Directory, how to plan for mail migration, as well as performance and network considerations when migrating mail.

At this point, the course transitions from planning for Office 365 to configuring Office 365. This begins with an introduction to the Office 365 clients, including mobile clients and Office online. Once you have a firm understanding of the Office 365 clients, you will then learn how to configure client connectivity to Office 365. This includes employing automatic client configuration, as well as how to configure the DNS records that must be maintained to support automatic client configuration. You will then examine Outlook clients and how to configure multi-factor authentication, as well as how to troubleshoot client connectivity issues.

The course then moves into the realm of Office 365 ProPlus deployments. You will learn how to manage client-driven installations, with a focus on Office 365 ProPlus licensing, activation, and update options. The course then examines how to manage centralized Office 365 ProPlus deployments, which involves configuring Office 365 ProPlus with the Office Deployment tool and deploying Office 365 ProPlus using Group Policy.

From there you will move into Office Telemetry, where you will learn about the data that is collected by Office Telemetry and how to plan for Telemetry. The course then examines how to install and configure Office Telemetry, as well as how to perform custom reporting in the Telemetry dashboard. The course concludes with a discussion on Windows Analytics, including how to configure Analytics and how to enroll devices in Analytics. This provides the foundation for using Analytics to assess your organization's readiness to deploy Office 365.

1.2. Microsoft 365 Tenant & Service Management

Microsoft 365 Tenant and Service Management focuses on learning how to plan, manage, and customize your organization's Microsoft 365 tenant and services. The course begins with an analysis of how to design your Microsoft 365 tenant. You will learn how to plan for a Microsoft 365 on-premises infrastructure, including preparing your organization for Microsoft 365 Enterprise, how to estimate your network bandwidth requirements, and best practices for integrating to Microsoft 365. We'll then cover how to plan your identity and authentication solution. This includes an examination of various authentication methods, including modern authentication, multi-factor authentication, pass-through authentication, and federated authentication. This discussion will end with a review of Active Directory federation services in Microsoft Azure, and how to restrict traffic in an AD FS deployment.

You will then transition from planning your Microsoft 365 tenant to configuring it. This begins with the various subscription options and component services that must be considered. You then move into setting up your organizational profile, managing tenant subscriptions, services, and add-ins. And to assist in this effort, you will be introduced to Microsoft FastTrack, and how this service can assist organizations in configuring their tenant and services.

With your Microsoft tenant and services in place, you will then learn how to manage these features following your initial deployment. Specifically, you will learn how to configure tenant roles and how to manage tenant health and services. This includes learning how to monitor your tenant health, how to develop an incident response plan, and how to request assistance from Microsoft.

At the conclusion of the course, you will be tasked with completing a series of hands-on lab exercises that enable you to practice what you just learned in the course. You will set up a Microsoft 365 tenant, manage Microsoft 365 users, groups, and administration, configure Rights Management and compliance, and monitor and troubleshoot Microsoft 365.

1.3. Microsoft 365 Identity Management

The Microsoft 365 Identity Management focuses on how to manage user security groups and licenses for cloud identities, and how to plan and implement identity synchronization, federated identities, applications, and external access. The course begins by examining how to manage user security groups and licenses for cloud identities. You will examine how to create user accounts in Microsoft 365, and how to manage those accounts as well as user licenses. The course then provides instruction on how to manage admin roles, security groups, and passwords in Microsoft 365. You will be introduced to identity management in Azure Active Directory, multi-factor authentication, and self-service password management.

The course then examines how to plan and implement identity synchronization. This begins with an introduction to identity synchronization, which includes an overview of Microsoft 365 authentication and provisioning options. You will then be introduced to directory synchronization and Azure AD Connect. From here you will learn how to effectively plan for and implement Azure AD Connect, including in both multi-forest scenarios and with pass-through authentication. Lastly, the course covers how to manage synchronized identities. This includes managing users and groups with directory synchronization, using Azure AD Connect synchronized security groups, and troubleshooting directory synchronization.

The course then transitions to federated identities. This begins with an introduction of federation identities, which includes an overview of Active Directory Federated Services, or AD FS, as well as an examination of how AD FS differs from Azure AD Connect password synchronization. You'll then look at single sign on options for Microsoft 365 and authentication flows with AD FS. The course then examines how to plan for and implement an AD FS deployment, which includes installing and configuring both AD FS and Web Application Proxy for AD FS. You'll also learn how to configure AD FS by using Azure AD Connect, as well as how to troubleshoot AD FS. Finally, you'll learn how to switch between federated authentication and password synchronization.

Lastly, the course covers how to implement applications and external access in Azure Active Directory. This begins with instruction on how to add and update applications, how to configure multi-tenant applications, and how to remove applications. With your applications in place, you'll then learn how to configure an Azure AD application proxy. This includes installing and registering a connector and publishing an on-premises app for remote access. The course concludes with a discussion on how to design solutions for external access, including licensing guidelines for an Azure AD business-to-

business collaboration. You will learn how to manage external access, how to create a collaboration user, and how to troubleshoot an Azure AD business-to-business collaboration.

Target Audience :

This course is designed for IT Professionals who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Objectives :

By actively participating in this course, you will learn about the following:

- Office 365 overview
- Moving your organization to Office 365
- Configuring Office 365
- Managing Office 365 ProPlus deployments
- Plan their Microsoft 365 on-premises infrastructure
- Plan their identity and authentication solution
- Plan and configure their Microsoft 365 experience
- Leverage Microsoft's FastTrack and partner services
- Implement their domain services
- Configure their Microsoft 365 tenant roles
- Manage their Microsoft 365 tenant health and services
- Manage user accounts and licenses in Microsoft 365
- Manage admin roles and security groups in Microsoft 365
- Plan and implement password management
- Manage Microsoft 365 authentication and provisioning options
- Plan for directory synchronization
- Plan and implement Azure AD Connect
- Manage synchronized identities
- Plan and implement an ADFS deployment
- Implement applications in Azure AD
- Configure Azure AD Application Proxy
- Design solutions for external access
- Manage their Microsoft 365 tenant health and services

Prerequisites :

- Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services
- A proficient understanding of general IT practices
- knowledge of written English, with course materials and the certification exam being in English.

2. MS-101 - Microsoft 365 Mobility and Security

Overview

This course is divided into 3 complementary parts :

2.1. Microsoft 365 Security Management

The Microsoft 365 Security Management course takes you on an extensive journey through the world of cloud security. The course begins by examining how to manage your security metrics. This begins by building a foundational understanding of the threat landscape that faces organizations today. The course introduces you to phishing, spoofing, spam and malware, account breaches, elevation of privileges, data exfiltration, data deletion, data spillage, and more. With this knowledge in place, you will then examine various security solutions that can address these threats, including Exchange Online Protection, Microsoft 365 Advanced Threat Protection, Microsoft 365 Threat Intelligence, and Advanced Security Management. The course then takes a deep dive into Azure AD Identity Protection, including how to enable it, how to configure it to detect vulnerabilities and risk events, and how to plan your investigation. This coverage of security metrics ends with an introduction to Microsoft Secure Score, which is a security analytics tool designed to help organizations understand what they have done to reduce the risk to their data, and show them what they can do to further reduce that risk.

With this foundational knowledge in place concerning today's threat landscape and the Microsoft 365 security solutions that are available to address those threats, the course then examines how to configure those solutions. This begins with an introduction to Exchange Online Protection (EOP), during which you will learn how EOP enables you to configure the anti-malware pipeline in Microsoft 365, as well as phishing and spoofing protection, zero-hour purge, and spoofing intelligence. The course then transitions to Advanced Threat Protection (ATP), where it examines how ATP expands on the protections provided by Exchange Online Protection by using its Safe Attachments and Safe Links features. The course then takes a deep dive into each of these features and examines how to create and manage safe attachment and safe links policies in

the Security and Compliance Center, as well as through Windows PowerShell. The course then identifies a variety of reports that are available to monitor your security status, including the Threat Protection Status report, the ATP message disposition report, the Malware Detections report, and much, much more.

The course concludes with an extensive examination of Microsoft 365 Threat Intelligence. Since Microsoft 365 hosts one of the largest networks in the world and manages content created on millions of devices, Microsoft has been able to build a vast repository of threat intelligence data, as well as the systems needed to spot patterns that correspond to attack behaviors and suspicious activity. Microsoft 365 Threat Intelligence is a collection of these insights, which can help organizations proactively find and eliminate threats. As such, the course examines how to plan for and implement Microsoft 365 Threat Intelligence. This includes using the Microsoft Intelligence Security Graph, the Security Dashboard, and Threat Explorer. You will then learn how to configure Advanced Threat Analytics (ATA) and how to manage ATA services. Finally, you will be instructed on how to implement your own cloud application security. This includes deploying cloud app security, controlling your cloud apps with policies, and troubleshooting your cloud app security status.

2.2. Microsoft 365 Compliance Management

This course introduces you to the world of Microsoft 365 compliance management. It begins with an introduction to the different solutions that are available in Microsoft 365 for data retention and data loss prevention. The course then takes a detailed look at the planning steps that are necessary to implement data retention policies and archiving rules. You will learn about the different approaches for single services with message retention management and a records center, as well as the new centralized approach of managing all Microsoft 365 data retention in the Security and Compliance Center.

You will then examine the steps needed to implement security and compliance requirements, such as proper organizational role management and the correct technical solutions that meet your business requirements. The course then analyzes how to protect your sensitive business data from being shared in ways that break your compliance rules, including implementing ethical walls and setting up data loss prevention policies.

Students are then introduced to the latest Microsoft 365 solutions for protecting your sensitive business data on client devices. You will learn how the Microsoft Information Protection solutions work to protect data and documents that leave your managed network perimeter and how to prevent users from accidental or intended sharing of business data with unsecure locations on their clients.

The course concludes by delving deep into eDiscovery investigations to track compliance breaches and manage compliance incidents with the Microsoft 365 tools from the Security and Compliance Center. The course examines how to manage and consolidate admin and user auditing log data from the Microsoft 365 services to provide complete compliance insight into your Microsoft 365 data and processes.

2.3. Microsoft 365 Device Management

Microsoft 365 Device Management focuses on how to establish Microsoft Intune, enroll devices to Intune, monitor the devices, and control what users can do from the enrolled devices by using conditional access policies. If you are already managing devices by using a traditional device management tool such as Configuration Manager, you will be interested to know how you can seamlessly move to modern management, in which devices are managed by Intune, and how you can benefit from new device management capabilities, such as compliance, conditional access, and Windows Autopilot to deploy new devices from the cloud.

The course begins by examining how to move from traditional management, where devices are managed by Configuration Manager, to modern management, where you can benefit from new capabilities such as device compliance and conditional access. This journey can begin by enabling co-management, which you can do in your current environment by adding Intune as an additional device management option. You can then move management of some Windows 10 devices to Intune, while all other devices remain managed by Configuration Manager. After you get confidence and experience with the benefits of modern management, you will probably want to move the management of your other devices to Intune as well.

The course then examines how you can monitor Windows 10 devices by using Windows Analytics. You will better understand the differences between quality updates and feature updates, as well as the Windows as a Service (WaaS) model, and when you must upgrade Windows 10 to a newer version to be supported by Microsoft. Although traditional, image-based deployment is still supported with Windows 10, many organizations will start exploring dynamic deployment and modern deployment options, such as Windows Autopilot.

The course concludes with an examination of how to implement Mobile Device Management (MDM). With Microsoft 365 you have two Mobile Device Management options: Intune and MDM for Office 365. You will learn how to perform an initial configuration of Intune so that it can manage Windows 10 and Android devices, as well as the additional preparation steps that are required for iOS devices. As Intune can manage only enrolled devices, you will learn how to enroll different device types. You will also learn also how to define a company baseline and use Intune to monitor device compliance against the baseline.

Targuet Audience :

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Objectives :

After completing this course, students will be able to:

- Manage Security Metrics
- Implement security solutions in Microsoft 365
- Plan and configure Azure AD identity protection
- Implement Microsoft Secure Score
- Implement Exchange Online Protection
- Implement Advanced Threat Protection
- Manage Safe Attachments and Safe Links
- Implement Microsoft 365 Threat Intelligence
- Use the Microsoft 365 Security Dashboard
- Configure Advanced Threat Analytics
- Implement cloud application security
- Understand Data Governance in Microsoft 365, including: Archiving, Retention, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 Message Encryption, Data Loss Prevention
- Implement In-Place Records Management in SharePoint
- Implement archiving and retention in Exchange
- Create retention policies in the Security and Compliance Center
- Plan their security and compliance needs
- Build ethical walls in Exchange Online
- Create a DLP Policy from a built-in template
- Create a custom DLP policy
- Create a DLP policy to protect documents
- Implement policy tips
- Manage retention in email
- Troubleshoot data governance
- Implement information protection and Advanced Implementation Protection
- Understand Windows Information Protections
- Search for content in the Security and Compliance Center
- Audit log investigations
- Manage advanced eDiscovery
- Plan for Co-management
- Prepare your Windows 10 devices for Co-management
- Transition from Configuration Manager to Intune
- Configure Microsoft Store for Business
- Plan for Mobile Application Management
- Plan your Windows 10 deployment strategy
- Plan your Windows 10 subscription activation strategy
- Resolve Windows 10 upgrade errors
- Implement Windows 10 Analytics
- Deploy Mobile Device Management
- Manage devices with Mobile Device Management
- Enroll devices to Mobile Device Management
- Manage device compliance

Prerequisites :

- completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration
- a proficient understanding of DNS and basic functional experience with Microsoft 365 services
- a proficient understanding of general IT practices
- knowledge of written English, with course materials and the certification exam being in English.

Duration and Price

Courses - Modules	Jours	CHF	CHF/j
MS-100 - Microsoft 365 Identity and Services	5	3'750.-	750.-
MS-101 - Microsoft 365 Mobility and Security	4	3'000.-	750.-

selon conditions générales. Le prix comprend toute la documentation distribuée.
Les cours se déroulent de 9 h 00 à 12 h 00 et 13 h 30 à 17 h 00

* Remise de 5 % au membre ADI, GRI, au diplômé(e) ISEIG CPF, titulaire du BFI, DFI ou certifié(e) MCSA, MCSE, MCSD formé(e) à l'ISEIG