MS100

Microsoft 365 Identity and Services

Microsoft 365 Identity and Services

MS100 - Version: 1

⏰ 5 days Course

Description:

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 tenant and service management, Microsoft 365 management, and Microsoft 365 identity management. In Microsoft 365 tenant and service management, you will examine all the key components that must be planned for when designing your Microsoft 365 tenant. Once this planning phase is complete, you will learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, and security groups. Finally, you will learn how to manage your tenant, which includes the configuration of tenant roles and managing your tenant health and services. With your Microsoft 365 tenant now firmly in place, you will examine the key components of Microsoft 365 management. This begins with an overview of Microsoft 365 product functionality, including Exchange Online, SharePoint Online, Microsoft Teams, Microsoft Power Platform, and device management. You will then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you will examine how to manage user-driven client installations of Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus) deployments. You will wrap up this section by learning how to configure Office Telemetry and Workplace Analytics. The course concludes with an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect. You will learn how to plan for and implement Azure AD Connect, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multi-factor authentication and self-service password management. This section wraps up with a comprehensive look at implementing application and external access. You will learn how to add and manage applications in Azure Active Directory, including how to configure multi-tenant applications. You will then examine how to

configure Azure AD Application Proxy, including how to install and register a connector and how to publish an on-premises app for remote access. Finally, you will examine how to design and manage solutions for external access. This includes licensing guidance for Azure AD B2B collaboration, creating a collaborative user, and troubleshooting a B2B collaboration.

Intended 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.

Prerequisites:

Before attending this course, students must have:
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.

Objectives:

Topics:

Plan your tenant in Microsoft 365

 • This module examines the key areas that organizations must plan for in order to create their Microsoft 365 tenant. These areas include subscription options, tenant components, and the overall migration process.
 • Learning objectives

- By the end of this module, you'll be able to:
- Determine which Microsoft 365 subscription offerings best suit your organization's requirements.
- Identify which Microsoft 365 component services satisfy your organizational needs.
- Identify the steps to successfully create a tenant for Microsoft 365.
- This module is part of these learning paths
- MS-100 Design your Microsoft 365 tenant
- Introduction
- Review the subscription options in Microsoft 365
- Examine the components in Microsoft 365 Enterprise Mobility and Security
- Determine the best subscription for your organization in Microsoft 365
- Plan a migration to Microsoft 365
- Knowledge check
- Summary

Plan your on-premises infrastructure for Microsoft 365

- This module examines the key areas that organizations must plan for in order to migrate their on-premises infrastructure to Microsoft 365.
- Learning objectives
- By the end of this module, you'll be able to:
- Prepare your organization to transition its on-premises deployment to Microsoft 365.
- Estimate your network's bandwidth.
- Describe best practices to employ when integrating your network to Microsoft 365.
- Identify the deployment strategies your company can use when implementing Microsoft 365 services.
- Prepare your Active Directory forest for directory synchronization.

Plan your identity and authentication solution for Microsoft 365

- This module examines the key areas that organizations must plan for in order to design the identity and authentication solutions they'll employ in their Microsoft 365 tenant.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe authentication behavior for Office client apps when they connect to Exchange Online, SharePoint Online, and Skype for Business Online.
- Explain how multi-factor authentication is supported in a Microsoft 365 deployment.
- Create a plan for directory synchronization and Azure AD Connect Pass-through authentication.
- Explore how password hash synchronization supports cloud authentication.
- Describe the issues, benefits, and best practices when implementing federated authentication using Active Directory Federation Services.
- Plan for Azure AD single sign-on.

Plan your supporting infrastructure for Microsoft 365

- This module examines the key areas that organizations must plan for in order to either move their Microsoft 365 service completely to the cloud or to hybridize their environment.
- Learning objectives
- By the end of this module, you'll be able to:
- Determine the best email migration or coexistence strategy for your organization.
- Create a file storage and collaboration strategy that is resilient and reliable.
- Prepare your organization to achieve the best experience using Microsoft Teams.

Plan hybrid requirements for your Microsoft 365 deployment

- This module examines the key areas that an organization must plan for in order to create hybrid environments for Exchange, SharePoint, and Skype for Business.
- Learning objectives
- By the end of this module, you'll be able to:

• Identify key considerations when planning a hybrid Exchange environment.

• Understand how planning your choices will affect your hybrid deployment.

• Describe the key planning options when designing a hybrid SharePoint environment.

• Identify the primary features of a hybrid deployment.

• Identify the infrastructure requirements for setting up a hybrid Skype for Business environment.

Plan your migration to Microsoft 365

• This module examines the key steps that must be completed in order to move an organization to Microsoft 365.

• Learning objectives

• By the end of this module, you'll be able to:

• Plan your organization's migration strategy to Microsoft 365.

• Analyze your organization's Active Directory and plan any necessary clean-up using the ID Fix tool.

• Determine which migration strategy to use to move your organization's mail, calendar, and contact information to the cloud.

• Describe the performance and network issues to consider when planning your organization's migration strategy.

Configure your Microsoft 365 experience

• This module examines each of the tasks that must be completed by an organization to successfully configure its Microsoft 365 experience.

• Learning objectives

• By the end of this module, you'll be able to:

• Configure your company's organization profile, which is essential for setting up for your company's tenant.

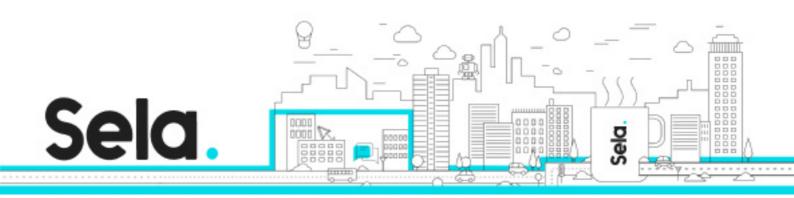• Maintain minimum subscription requirements for your company.

• Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.

• Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.

Manage user accounts and licenses in Microsoft 365

• This module provides instruction on how to manage user accounts and licenses in Microsoft 365, create and manage user accounts, assign Microsoft 365 licenses to users, and recover deleted user accounts.

• Learning objectives

• By the end of this module, you'll be able to:

• Identify which user identity model best suited for your organization.

• Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.

• Manage user accounts and licenses in Microsoft 365.

• Recover deleted user accounts in Microsoft 365.

• Perform bulk user maintenance in Azure Active Directory.

Manage groups in Microsoft 365

• This module provides instruction on how to create groups for distributing email to multiple users within Exchange Online. It also explains how to create groups to support collaboration in SharePoint Online.

• Learning objectives

• By the end of this module, you'll be able to:

• Describe the various types of groups available in Microsoft 365.

• Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.

• Create and manage groups in Exchange Online and SharePoint Online.

Add a custom domain in Microsoft 365

 • This module provides instruction on how to add a custom domain to your Microsoft 365 deployment. It also examines the DNS requirements that are necessary to support a new domain.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Identify the factors that must be considered when adding a custom domain to Microsoft 365.
 • Plan the DNS zones used in a custom domain.
 • Plan the DNS record requirements for a custom domain.
 • Add a custom domain to your Microsoft 365 deployment.

Configure client connectivity to Microsoft 365

 • This module examines how clients connect to Microsoft 365. It also provides instruction on how to configure name resolution and Outlook clients, and how to troubleshoot client connectivity.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
 • Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
 • Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
 • Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

Configure administrative roles in Microsoft 365

 • This module examines the key functionality that's available in the more commonly used Microsoft 365 admin roles. It also provides instruction on how to configure these roles.

- Learning objectives
- By the end of this module, you'll be able to:
- Describe the Azure RBAC permission model used in Microsoft 365.
- Describe the most common Microsoft 365 admin roles.
- Identify the key tasks performed by users who are assigned to the common Microsoft 365 admin roles.
- Delegate admin roles to partners.
- Manage permissions using administrative units in Azure Active Directory.
- Elevate privileges to access admin centers by using Azure AD Privileged Identity Management.

Manage tenant health and services in Microsoft 365

- This module examines how to monitor your organization's transition to Microsoft 365 using Microsoft 365 tools. It also examines how to develop an incident response plan and request assistance from Microsoft.
- Learning objectives
- By the end of this module, you'll be able to:
- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues.

Deploy Microsoft 365 Apps for enterprise

- This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.
- Learning objectives

- By the end of this module, you'll be able to:
- Describe the Microsoft 365 Apps for enterprise functionality.
- Configure the Readiness Toolkit.
- Plan a deployment strategy for Microsoft 365 Apps for enterprise.
- Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- Deploy Microsoft 365 Apps for enterprise using group policy.
- Describe how to manage Microsoft 365 Apps for enterprise updates.
- Determine which update channel and application method applies for your organization.

Manage secure user access in Microsoft 365

- This module examines various password-related tasks for user and admin accounts, such as creating and configuring password policies, configuring self-service password management, configuring multifactor authentication, and implementing entitlement packages and conditional access policies.
- Learning objectives
- By the end of this module, you'll be able to:
- Manage user passwords
- Describe pass-through authentication
- Enable multifactor authentication
- Describe self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and perform an access review

Analyze your Microsoft 365 workplace data using Microsoft Viva Insights

- This module examines the workplace analytical features of Microsoft Viva Insights, including how it works, and how it generates insights and improves collaboration within an organization.
- Learning objectives
- After completing this module, you'll be able to:
- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- Discover the sources of data used in Microsoft Viva Insights.
- Explain the high-level insights available through Microsoft Viva Insights.
- Create custom analysis with Microsoft Viva Insights.
- Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.

Explore Exchange Online as a Microsoft 365 Enterprise Administrator

- This module examines the key features of Exchange Online, including how to create and manage recipients, anti-malware policies, and anti-spam policies, and how to migrate mailboxes in a hybrid deployment.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe how mail flows through a Microsoft 365 deployment
- Describe the most common recipient types that are available in Exchange Online
- Manage anti-malware and anti-spam policies in Exchange Online
- Describe migration and coexistence strategies and understand the differences between them
- Select the right mail migration strategy for your organization
- Determine when you want to change the DNS MX record for a domain in a Microsoft 365 migration to point to Exchange Online
- Describe the different ways to migrate mailboxes to Microsoft 365 in a hybrid Exchange environment

Explore SharePoint Online as a Microsoft 365 Enterprise Administrator

• This module examines the key features of SharePoint Online, including how it enables organizations to manage local sites and hub sites, recover deleted content, provide anti-malware protection, and facilitate external sharing.

• Learning objectives

• By the end of this module, you'll be able to:

• Determine the out-of-the-box permission levels that your organization should use in SharePoint Online when creating sites and segregating and restricting access to content that is considered confidential or proprietary

• Plan a migration strategy to migrate file shares to SharePoint Online and OneDrive

• Identify the options available in SharePoint Online to maintain and recover content that has either been deleted or misplaced in your organization's intranet

• Describe the different options that provide anti-malware protection in SharePoint Online

• Plan a hybrid SharePoint Online deployment

Explore Microsoft Teams as a Microsoft 365 Enterprise Administrator

• This module examines the key features of Microsoft Teams and provides instruction on how to manage authentication and access to Teams, implement guest access, manage audio conferencing, and implement Microsoft Teams Phone.

• Learning objectives

• By the end of this module, you'll be able to:

• Describe basic Teams functionality and the infrastructure that supports its goals

• Describe how Teams compares to the other collaboration apps in Microsoft 365

• Provide Teams access by managing user licenses in the Microsoft 365 admin center and PowerShell

• Describe the functionality provided by Guess access in Microsoft Teams

• Describe audio conferencing functionality that is available in Microsoft Teams

• Assign an audio conferencing license and a conference ID to each user to support audio conferencing

- Manage user settings for audio conferencing
- Select a voice solution using Microsoft Teams Phone
- Manage your organizational settings in Microsoft Teams

Explore Microsoft Power Platform as a Microsoft 365 Enterprise Administrator

- This module examines the key features of Microsoft's Power Platform and provides an introduction to the components that make up the Microsoft Power Platform product family.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe what the Microsoft Power Platform is
- Identify the components that make up the Microsoft Power Platform product family
- Implement the Microsoft Power Platform Center of Excellence starter kit
- Describe the basic features of the Microsoft Power Platform admin center
- Describe the Microsoft Power Platform security model

Create apps as a Microsoft 365 Enterprise Administrator with Power Apps

- This module examines the key features of Power Apps and provides instruction on how to manage the Power Apps environment, connect to data sources, and create, test, monitor, and run a Power App.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe Power Apps functionality, including its business impact and primary components
- Manage the Power Apps environment in the Power Apps admin center and with Windows PowerShell
- Describe how Power Apps connects to data sources
- Create, test, and monitor a canvas Power App
- Run canvas and mobile Power Apps

Create flows as a Microsoft 365 Enterprise Administrator with Power Automate

 • This module examines the key features of Power Platform and provides instruction on how to administer Power Platform flows, connect flows to data sources, and create and run flows.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Describe what Power Automate is and how it is used by organizations
 • Describe the types of flows you can create and the basic structure of flows
 • Administer Power Automate licensing and environments
 • Describe how flows connect to data sources
 • Build a basic flow using Power Automate
 • Run a flow in Power Automate, Teams, and SharePoint

Create reports and dashboards as a Microsoft 365 Enterprise Administrator with Power BI

 • This module examines the key features of Power BI (Business Intelligence) and provides instruction on how to create reports, dashboards, and visualizations, connect Power BI to data sources, and administer and share your results.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Describe what Power BI is and how it's used by organizations
 • Describe how Power BI connects to data sources
 • Build and share a basic Power BI report and dashboard
 • Administer Power BI permissions, licensing, and row level security

Create chatbots as a Microsoft 365 Enterprise Administrator with Power Virtual Agents

• This module introduces the key features of Power Virtual Agents and provides instruction on how to create powerful bots using Power Virtual Agents' guided, no-code graphical user interface.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Explain the purpose of Power Virtual Agents within the Power Platform.
 • Explain how Power Agents enable teams to easily create powerful bots.
 • Describe key features of Power Virtual Agents.
 • Create a bot using Power Virtual Agents.

Explore identity synchronization

 • This module examines identity synchronization using Azure AD Connect and explores the authentication and provisioning options that can be used and the inner-workings of directory synchronization.
 • Learning objectives
 • By the end of this module, you'll be able to:
 • Describe the Microsoft 365 authentication and provisioning options
 • Explain directory synchronization
 • Explain how Azure AD Connect enables coexistence between your on-premises Active Directory environment and Microsoft 365

Prepare for identity synchronization to Microsoft 365

 • This module examines all the planning aspects that must be considered when implementing directory synchronization between on-premises Active Directory and Microsoft 365.
 • Learning objectives
 • By the end of this module, you'll be able to:

- Identify the tasks necessary to configure your Azure Active Directory environment.
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- Identify the features of Azure AD Connect sync and Azure AD Connect Cloud Sync.
- Choose which directory synchronization best fits your environment and business needs.

Implement directory synchronization tools

- This module examines the Azure AD Connect installation requirements, the options for installing and configuring the tool, and how to monitor synchronization services using Azure AD Connect Health.
- Learning objectives
- By the end of this module, you'll be able to:
- Configure Azure AD Connect prerequisites
- Set up Azure AD Connect and Azure AD Connect Cloud Sync
- Monitor synchronization services using Azure AD Connect Health
- This module examines how to manage user identities when Azure AD Connect is configured, how to manage users and groups in Microsoft 365 with Azure AD Connect, and how to maintain directory synchronization.
- Ensure your users synchronize efficiently
- Deploy Azure AD Connect
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization using various troubleshooting tasks and tools

Implement applications in Azure AD

- This module provides instruction on how to register applications in Azure AD, update applications within the Azure AD consent framework, configure multi-tenant applications, manage OAuth application requests, and monitor app governance.

- Learning objectives
- By the end of this module, you'll be able to:
- Register an application or service within your Azure AD tenant
- Update an application within the Azure AD consent framework
- Modify the configuration of a single-tenant application to make it a multi-tenant application
- Manage OAuth application requests
- Monitor app governance for OAuth-enabled apps

Configure Azure AD Application Proxy

- This module examines Azure AD Application Proxy and connectors, how to install and register a connector, and how to publish an on-premises app for remote access.
- Learning objectives
- By the end of this module, you'll be able to:
- Describe the benefits of Azure AD Application Proxy, the type of applications that work with it, and how it works
- Identify Azure AD Application Proxy prerequisites
- Install and register a connector and verify that it installed correctly
- Publish an on-premises app for remote access and test the published app to verify that it functions correctly

Explore solutions for external access

- This module examines how to enable external access across various solutions, including Azure Active Directory Business to Business (B2B) collaboration, Microsoft 365, Microsoft Teams, and Customer Lockbox.
- Learning objectives
- By the end of this module, you'll be able to:
- Identify the features of external access with Azure Active Directory B2B collaboration.

 • Explain the difference between Microsoft 365 external access and Azure Active Directory B2B collaboration.

 • Explain the attributes of a collaborative user.

 • Demonstrate Azure Active Directory B2B collaboration.

 • Identify the differences between external access and guest access using Microsoft Teams.

 • Describe usage scenarios for Customer Lockbox requests.