Microsoft Partner

FIREFLY

CONTACT US

Microsoft 365 Mobility and Security

Enterprise Administrator Expert

DURATION: 5 DAYS COURSE CODE: MS-101 FORMAT: LECTURE/LAB

WHY FIREFLY

Firefly is trusted by customers, technology vendors and channel partners around the world to deliver highly effective, immersive educational experiences. Our innovative, role-based Microsoft training covers all of the latest certifications, from Azure to Server 2016 to SQL to the modern desktop, and is designed engineers the skills they need to remain relevant in today's multicloud world.

WHO SHOULD ATTEND

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

Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.

Microsoft 365 Security Management	Microsoft 365 Compliance Management	Microsoft 365 Device Management

LEARNING OBJECTIVES

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

Implement 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

MS-101T01-A: Microsoft 365 Security Management

DESCRIPTION

Learn about Microsoft 365 Security Management, including how to manage your security metrics, how to enable Azure AD Identity Protection, how to configure your Microsoft 365 security services, and user Microsoft 365 Threat Intelligence.

COURSE OUTLINE

1. Designing your Microsoft 365 Tenant
   - Planning a Microsoft 365 On-premises infrastructure
   - Planning Your Identity and Authentication Solution
2. Configuring your Microsoft 365 Tenant
   - Planning your Microsoft 365 Experience
   - Configuring your Microsoft 365 Experience
   - Leveraging FastTrack and Partner Services
   - Implementing Your Domain Services
3. Managing your Microsoft 365 Tenant
   - Configuring Tenant Roles
   - Managing Tenant Health and Services
4. Hands-On Lab

LABS

Managing Microsoft 365 Security

1. Setting up your lab environment
2. Editing an ATP Safe Links policy and create a Safe Attachment policy
3. Enabling and installing the ATA Center

MS-101T02-A: Microsoft 365 Compliance Management

DESCRIPTION

Learn about Microsoft 365 Compliance Management, including data retention and data loss prevention solutions in Microsoft 365, archiving and retention in Microsoft 365, implementing and managing data governance, and managing search and investigations.

COURSE OUTLINE

1. Introduction to Data Governance in Microsoft 365
   - Introduction to Archiving in Microsoft 365
   - Introduction to Retention in Microsoft 365
   - Introduction to Information Rights Management
   - Introduction to Secure Multipurpose Internet Mail Extension
   - Introduction to Office 365 Message Encryption
   - Introduction to Data Loss Prevention
2. Archiving and Retention in Microsoft 365
   - In-Place Records Management in SharePoint
   - Archiving and Retention in Exchange
   - Retention Policies in the SCC
   - Implementing Your Domain Services
3. Implementing Data Governance in Microsoft 365 Intelligence
   - Planning Your Security and Compliance Needs
   - Building Ethical Walls in Exchange Online
   - Creating a Simple DLP Policy from a Built-in Template
   - Creating a Custom DLP Policy
   - Creating a DLP Policy to Protect Documents
   - Working with Policy Tips
4. Managing Data Governance in Microsoft 365
   - Managing Retention in Email
   - Troubleshooting Data Governance
   - Implementing Information Protection
   - Implementing Advanced Information Protection
   - Introduction to Windows Information Protection
5. Managing Search and Investigations
   - Searching for Content in the Security and Compliance Center
   - Auditing Log Investigations
   - Managing Advanced eDiscovery
6. 6: Hands-On Lab
   - Searching for Content in the Security and Compliance

LABS

1. Setting Up your Lab Environment
   - Initialize Compliance in Your Organization
2. Archiving and Retention in Microsoft 365
   - Configure Retention Tags and Policies
   - Configure AIP and WIP
3. Implementing Data Governance
   - Testing DLP Policies
   - Using Azure Information Protection
   - Using Windows Information Protection
4. Verify Your Data Governance Policies
   - Investigate your Microsoft 365 Data

MS-101T03-A: Microsoft 365 Device Management

DESCRIPTION

This course introduces you to the world of Microsoft 365 device management - from establishing Microsoft Intune, to enrolling devices to Intune, to monitoring the devices, to controlling 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.

COURSE OUTLINE

1. Planning for Device Management
   - Introduction to Co-management
   - Preparing Your Windows 10 Devices for Co-management
   - Transitioning from Configuration Manager to Intune
   - Introduction Microsoft Store for Business
   - Planning for Mobile Application Management
2. Planning Your Windows 10 Deployment Strategy
   - Windows 10 Deployment Scenarios
   - Planning Your Windows 10 Subscription Activation Strategy
   - Resolving Windows 10 Upgrade Errors
   - Introduction to Windows Analytics
3. Implementing Mobile Device Management
   - Planning Mobile Device Management
   - Deploying Mobile Device Management
   - Enrolling Devices to MDM
   - Managing Device Compliance
4. Hands-On Lab

LABS

1. Working with Microsoft Store for Business
   - Provisioning and managing the Microsoft Store for Business
   - Using the Microsoft Store for Business
2. Managing Devices by using Intune
   - Obtain Intune and enable device management
   - Configure Azure AD for Intune
   - Create Intune policies
   - Enroll a Windows 10 device
   - Manage and monitor a device in Intune