Protecting Modern Desktops and Devices (MD-101.3)

Modality: On Demand

Duration: 12 Hours

About this course:

Security in a workplace is an important issue in these times. Nowadays, demand for mobility has increased. By this we mean that the IT is now required by more and more organizations to tether all the devices apart from the working PC, with each other. The Desktop Administrator should be able to interconnect the devices of other users like tablets, phones, and computers. The computer must be made compatible to connect with whichever device that is needed to be connected, regardless of if it is employee's personal or the company's device. This is where the issue of security of data and protection of devices comes forth. IT has to responsibly assure the security of all the users.

This is where this course comes in handy. In this course, the student will be taught about the different aspects of security and its maintenance in the modern management. These aspects include authentication, identities, access to the data, and alongside this, the security of these aspects. The student will be taught on how to regulate and manage the issues in here. There will be an introduction to the popular cloud-based identity and access regulatory service, Azure Active Directory as well as on the usage of Microsoft Intune. Microsoft Intune is also a helpful cloud-based management system which protects data and devices from the compliance policies. In the end, the course will adequately cover different topics of Azure Information Protection service and security software of Windows Defender Advanced Threat Protection. The course will also teach the incorporation method of the learned skills too.

Learning Objectives:

The course has the following learning objectives:

- Explaining the basics, importance and advantages of Azure Active Directory
- Regulation of users using Azure AD by using Active Directory Domain Services
- Incorporating in the system the authentication technology of Windows Hello for Business
- Setting up a conditional access to the system for the users in order to follow the compliance policies
- Explaining the different methods and tools used for the security of data and devices
- Incorporate the security system of Windows Defender Advanced Threat Protection

Audience:

This course is a suitable certification for IT professionals and Windows Administrators

Requirements:

It is important that the Desktop administrator has a sound knowledge of M365 workloads. The administrator also needs to have a profound experience and expert skills in the execution, setting up,

and maintaining of Windows 10 as well as the non-Windows devices. It is highly recommended that you must have training in the Windows 10 courses of (MD100), MD101.1, and MD101.2 before starting this course.

Course Outline:

Managing Authentication in Azure AD

- Azure AD Overview
- Managing identites in Azure AD
- Protecting identities in Azure AD
- Managing device authentication
- Enabling corporate access
- Practice Lab
- Module Assessment

Managing Devices and Device Policies

- Microsoft Intune Overview
- Managing devices with Intune
- Implement device compliance policies
- Practice Lab
- Module Assessment

Managing Security

- Implement device data protection
- Managing Windows Defender ATP
- Managing Windows Defender in Windows 10
- Practice Lab
- Module Assessment

Course Conclusion

- Final Exam