

Exam 70-797: Configuring Windows Devices (pilot) – Skills Measured

Audience Profile

This exam validates a candidate's fundamental knowledge and skills for building solid identities, protection of content (data loss protection), mobile device management policy, virtualization with Hyper-V, application management using the Company Portal and the Windows Store. Candidates will be evaluated on Windows 10 security and integrated Azure features.

In addition to their professional experience, candidates who take this exam should already have the following technical knowledge:

- Experience with Windows desktop administration, maintenance, and troubleshooting
- Basic experience and understanding of Windows networking technologies
- Introductory-level knowledge of Active Directory and Microsoft Intune

Candidates can take this exam and meet the prerequisites by obtaining equivalent knowledge and skills through practical experience as a Windows device support technician or a Windows device system administrator.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: In most cases, exams do NOT cover preview features, and some features will only be added to an exam when they are GA (General Availability).

Manage identity (13%)

Support Windows Store and cloud apps

- install and manage software by using Microsoft Office 365 and Windows Store apps, sideload apps by using Microsoft Intune, sideload apps into online and offline images, deeplink apps by using Microsoft Intune, integrate Microsoft account including personalization settings

Support authentication and authorization

- identifying and resolving issues related to the following: Multi-factor authentication including certificates, Microsoft Passport, virtual smart cards, picture passwords, and

biometrics; workgroup vs. domain, Homegroup, computer and user authentication including secure channel, account policies, credential caching, and Credential Manager; local account vs. Microsoft account; Workplace Join; Configuring Windows Hello

Plan desktop and device deployment (13%)

Migrate and configure user data

- migrate user profiles; configure folder location; configure profiles including profile version, local, roaming, and mandatory

Configure Hyper-V

- create and configure virtual machines including integration services, create and manage checkpoints, create and configure virtual switches, create and configure virtual disks, move a virtual machine's storage

Configure mobility options

- configure offline file policies, configure power policies, configure Windows To Go, configure sync options, configure Wi-Fi direct, files, powercfg, Sync Center

Configure security for mobile devices

- configure BitLocker, configure startup key storage

Plan and implement a Microsoft Intune device management solution (11%)

Support mobile devices

- support mobile device policies including security policies, remote access, and remote wipe; support mobile access and data synchronization including Work Folders and Sync Center; support broadband connectivity including broadband tethering and metered networks; support Mobile Device Management by using Microsoft Intune, including Windows Phone, iOS, and Android

Deploy software updates by using Microsoft Intune

- use reports and In-Console Monitoring to identify required updates, approve or decline updates, configure automatic approval settings, configure deadlines for update installations, deploy third-party updates

Manage devices with Microsoft Intune

- provision user accounts, enroll devices, view and manage all managed devices, configure the Microsoft Intune subscriptions, configure the Microsoft Intune connector site system role, manage user and computer groups, configure monitoring and alerts, manage policies, manage remote computers

Configure networking (11%)

Configure IP settings

- configure name resolution, connect to a network, configure network locations

Configure networking settings

- connect to a wireless network, manage preferred wireless networks, configure network adapters, configure location-aware printing

Configure and maintain network security

- configure Windows Firewall, configure Windows Firewall with Advanced Security, configure connection security rules (IPsec), configure authenticated exceptions, configure network discovery

Configure storage (10%)

Support data storage

- identifying and resolving issues related to the following: DFS client including caching settings, storage spaces including capacity and fault tolerance, OneDrive

Support data security

- identifying and resolving issues related to the following: Permissions including share, NTFS, and Dynamic Access Control (DAC); Encrypting File System (EFS) including Data Recovery Agent; access to removable media; BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM)

Manage data access and protection (11%)

Configure shared resources

- configure shared folder permissions, configure HomeGroup settings, configure libraries, configure shared printers, configure OneDrive

Configure file and folder access

- encrypt files and folders by using EFS, configure NTFS permissions, configure disk quotas, configure file access auditing Configure authentication and authorization

Manage remote access (10%)

Configure remote connections

- configure remote authentication, configure Remote Desktop settings, configure VPN connections and authentication, enable VPN reconnect, configure broadband tethering

Configure mobility options

- configure offline file policies, configure power policies, configure Windows To Go, configure sync options, configure Wi-Fi direct

Manage apps (11%)

Deploy and manage Azure RemoteApp

- configure RemoteApp and Desktop Connections settings, configure Group Policy Objects (GPOs) for signed packages, subscribe to the Azure RemoteApp and Desktop Connections feeds, export and import Azure RemoteApp configurations, support iOS and Android, configure remote desktop web access for Azure RemoteApp distribution

Support desktop apps

- the following support considerations including: Desktop app compatibility using Application Compatibility Toolkit (ACT) including shims and compatibility database; desktop application co-existence using Hyper-V, Azure RemoteApp, and App-V; installation and configuration of User Experience Virtualization (UE-V); deploy desktop apps by using Microsoft Intune

Manage updates and recovery (10%)

Configure system recovery

- configure a recovery drive, configure system restore, perform a refresh or recycle, perform a driver rollback, configure restore points

Configure file recovery

- restore previous versions of files and folders, configure File History, recover files from OneDrive

Configure and manage updates

- configure update settings, configure Windows Update policies, manage update history, roll back updates, update Windows Store apps