INFORMATION TECHNOLOGY

Comprehensive Guide to Microsoft Exam 70-697: Mastering Windows 10 Device Configuration in the Enterprise

Published: December 28, 2026 | Tags: 70 697 | Windows 10 | Microsoft Certification | Intune | Azure AD | Device Management

The landscape of enterprise computing underwent a seismic shift with the introduction of Windows 10, moving away from static, perimeter-based security toward a more fluid, cloud-integrated model. At the heart of this transition was **Microsoft Exam 70-697: Configuring Windows Devices**. This exam was designed to validate the skills of IT professionals in managing Windows 10 devices in a variety of environments, including physical hardware, virtual machines, and cloud-based infrastructures. As a core component of the Microsoft Certified Solutions Associate (MCSA) Windows 10 certification, 70-697 focused heavily on identity, cloud services, and mobile device management (MDM).

The Strategic Importance of Windows 10 Configuration

In the modern enterprise, configuring a device is no longer just about installing an operating system and joining it to a local domain. It involves a holistic approach to **Identity Management**, **Data Security**, and **Application Lifecycle Management**. The 70-697 curriculum was pioneering because it integrated Microsoft Azure and Intune directly into the desktop administration workflow. This shift recognized that the modern workforce is mobile and requires secure access to corporate resources from any location, on any device.

Core Objective Domains

The exam and the subsequent field practices are divided into several critical domains that every Windows administrator must master:

- Manage Identity: Understanding the nuances between Microsoft Accounts, Local Accounts, and Azure Active Directory (Azure AD) identities.
- Plan Desktop and Device Deployment: Moving beyond traditional imaging to dynamic provisioning and migration.
- Configure Networking: Managing IP settings, name resolution, and remote connectivity protocols like DirectAccess and VPNs.
- Configure Storage: Implementing NTFS, ReFS, and cloud-storage solutions like OneDrive for Business.

- Manage Data Access and Protection: Utilizing BitLocker, EFS, and Windows Information Protection (WIP).
- Manage Remote Access: Configuring remote desktop and remote management tools.
- Manage Apps: Deploying and securing applications via the Microsoft Store for Business and sideloading.
- Manage Updates and Recovery: Implementing Windows Update for Business and recovery strategies.

Deep Dive into Identity and Cloud Integration

Identity is the new perimeter. Exam 70-697 places a significant emphasis on how users authenticate. Traditional Active Directory Domain Services (AD DS) remain relevant, but the integration with **Azure Active Directory (Azure AD)** is what defines modern Windows management.

Azure AD Join vs. Domain Join

Understanding when to use a traditional Domain Join versus an Azure AD Join is fundamental. Traditional Domain Join relies on a local domain controller and is ideal for machines that stay within the corporate network. **Azure AD Join**, conversely, allows for seamless authentication to cloud resources like Office 365 without needing a VPN to reach a local domain controller. It supports **Single Sign-On (SSO)** and allows for the automatic enrollment of devices into MDM solutions like Microsoft Intune.

Feature	Traditional Domain Join (AD	Azure AD Join	Workplace Join (Registered)
Primary Identity	On-premises AD Account	Azure AD Cloud Account	Microsoft Account / Azure AD
Authentication	Kerberos / NTLM	Modern Auth (OAuth2/SAML)	Device Registration Service
GPO Support	Full Support	Limited (via MDM)	No GPO Support
Primary Use Case	Corporate-owned, on-prem	Corporate-owned, mobile/cloud	BYOD (Bring Your Own Device)

Microsoft Intune and MDM Policies

Configuring Windows devices frequently involves **Mobile Device Management (MDM)**. Microsoft Intune allows administrators to push configurations, security settings, and applications over the air. This replaces or augments Group Policy Objects (GPOs) for devices that aren't always connected to the local network. Key components include **Configuration Profiles**, which define settings for Wi-Fi, VPN, and security baselines, and **Compliance Policies**, which ensure a device meets specific security requirements (like having BitLocker enabled) before accessing corporate data.

Technical Analysis of Data Protection Mechanisms

Data security on a Windows 10 device is multi-layered. The 70-697 objectives require a deep technical understanding of how encryption and file permissions interact to protect sensitive information.

BitLocker Drive Encryption (BDE)

BitLocker provides full-volume encryption. It typically leverages a **Trusted Platform Module (TPM)** , a specialized chip on the motherboard that stores the encryption keys. The technical workflow for BitLocker involves:

1. Initialization: Validating the TPM and ensuring the BIOS/UEFI is secure.
2. Encryption: Using the AES-XTS algorithm to encrypt the entire disk sector by sector.
3. Key Escrow: Backing up the recovery key to Azure AD, Active Directory, or a file.

Administrators must be proficient with the command-line tool and the PowerShell cmdlet to audit and manage encryption states across a fleet of devices.

Windows Information Protection (WIP)

Formerly known as Enterprise Data Protection (EDP), WIP helps protect against potential data leakage without otherwise interfering with the employee experience. WIP differentiates between personal and corporate data. If a user attempts to copy data from a corporate document into a personal application (like a public social media site), WIP can block the action or log the event based on the defined policy.

NTFS vs. ReFS: Choosing the Right File System

While NTFS remains the standard, **Resilient File System (ReFS)** was introduced to maximize data availability and integrity. In the context of 70-697, understanding the limitations of each is crucial for storage configuration.

Feature	NTFS	ReFS
Maximum Volume Size	256 TB	1 Yottabyte
File Compression	Supported	Not Supported
Disk Quotas	Supported	Not Supported
Self-Healing	Manual (Chkdsk)	Automatic (Integrity Streams)
Encryption	EFS Supported	No EFS Support

Networking and Remote Connectivity Solutions

Configuring Windows devices requires a robust understanding of how those devices communicate. This includes both local networking (IPv4/IPv6) and remote access technologies.

DirectAccess vs. VPN

DirectAccess provides a seamless, always-on remote connection. It uses IPsec and IPv6 to create a bidirectional tunnel between the client and the corporate network. Because it connects before the user logs in, it allows IT to manage the device even when it's not on-site. However, it requires specific infrastructure (Windows Server 2012 R2 or later and Enterprise edition clients). **VPNs (Virtual Private Networks)**, particularly **IKEv2**-based VPNs, offer similar functionality but usually require a manual trigger or a "Triggered VPN" configuration within Windows 10.

Transition Technologies

As the world moves toward IPv6, Windows 10 utilizes several transition technologies to ensure connectivity over IPv4-only networks:

- Teredo: Encapsulates IPv6 packets within IPv4 UDP packets to allow communication through NATs.
- 6to4: Allows IPv6 packets to be transmitted over an IPv4 network using protocol 41.
- ISATAP: Intra-Site Automatic Tunnel Addressing Protocol, used for communication within a site between IPv6/IPv4 nodes.

Practical Implementation: A Step-by-Step Field Guide

Implementing the concepts from Exam 70-697 requires a systematic approach. Below is a procedural guide for a common enterprise task: **Provisioning a New Windows 10 Device with Azure AD and Intune.**

Step 1: Preparing the Tenant

Before enrolling devices, the Azure AD tenant must be configured. This includes setting the **MDM User Scope** to "All" or a specific group to ensure that when a user joins their device to Azure AD, it automatically enrolls in Intune.

Step 2: Configuring Windows Autopilot

Windows Autopilot is a collection of technologies used to set up and pre-configure new devices. To use Autopilot, the administrator must harvest the **Hardware ID (Hardware Hash)** from the device and upload it to the Microsoft Store for Business or the Intune portal. An **Autopilot Deployment Profile** is then assigned, which can skip the Privacy Settings, EULA, and Account Setup screens

for the end user.

Step 3: Defining Configuration Profiles

In the Intune console, create a **Configuration Profile**. For example, to enforce BitLocker, you would:

1. Navigate to Device Configuration > Profiles > Create Profile.
2. Select Platform: Windows 10 and later and Profile Type: Endpoint Protection.
3. Under Windows Encryption, set "Encrypt devices" to "Require".
4. Configure TPM settings and recovery key backup options.

Step 4: End-User Out-of-Box Experience (OOBE)

When the user receives the new device, they simply power it on, connect to Wi-Fi, and enter their corporate email and password. Windows Autopilot takes over, joins the device to Azure AD, enrolls it in Intune, and applies all pre-defined configuration profiles and applications.

Case Studies: Troubleshooting Common Configuration Failures

In real-world scenarios, configuration often meets resistance from legacy hardware or network constraints. Analyzing these failures is a core skill for any senior technical writer or administrator.

Scenario A: BitLocker Encryption Fails to Initialize

Problem: A fleet of laptops is failing to encrypt. The error log indicates "TPM not found" or "TPM not initialized".

Solution: Check the BIOS/UEFI settings to ensure the TPM is set to "Enabled" and "Active". If using older hardware, verify if the TPM version is 1.2 or 2.0. Windows 10 highly prefers TPM 2.0. Additionally, ensure the drive has a **System Partition** separate from the boot partition, as BitLocker requires an unencrypted partition for boot files.

Scenario B: Azure AD Join Issues (Error 0x801c0003)

Problem: Users receive error 0x801c0003 when attempting to join a device to Azure AD.

Solution: This error typically relates to the user's permission to join devices. Navigate to the Azure Portal, go to *Azure Active Directory* > *Devices* > *Device Settings*, and verify that "Users may join devices to Azure AD" is enabled and that the user hasn't exceeded the "Maximum number of devices per user" limit (default is 50).

Application Management and Modern Distribution

Exam 70-697 covers the transition from legacy and installers to modern app packages. The **Micro**

soft Store for Business allows organizations to find, acquire, manage, and distribute apps in volume. Organizations can also **Sideload** apps, which means installing them directly without using the Store. This is common for internally developed Line-of-Business (LOB) apps. To sideload, the device must have the sideloading policy enabled via GPO or MDM, and the app must be signed by a certificate trusted by the device.

The Long-Term Impact of 70-697 Knowledge

While Microsoft has retired the 70-697 exam in favor of the MD-100 (Windows Client) and MD-101 (Managing Modern Desktops) - which have now evolved into the **MD-102 (Endpoint Administrator)** - the core principles remain identical. The shift toward cloud-based management, identity-centric security, and automated provisioning that 70-697 introduced is now the industry standard. Administrators who mastered the 70-697 objectives are well-positioned to manage modern endpoints, as the underlying architecture of Azure AD Join, Intune policies, and BitLocker orchestration has only become more refined over time.

Understanding the "Configuring Windows Devices" framework is not just about passing a test; it is about building a scalable, secure, and user-friendly computing environment. By focusing on the integration of local power and cloud flexibility, IT professionals can ensure that their organizations remain resilient in an ever-changing digital landscape. The technical depth required to manage these systems - from understanding the nuances of the **Windows Boot Manager** to the complexities of **Graph API** integrations in Intune - marks the difference between a technician and a true systems engineer.