TestOut Client Pro – English 7.0.x

Objective Mappings:

TestOut Client Pro
Microsoft MD-100
Microsoft MD-101

Revised: 2021-08-10

Powered by LABSIM

Contents

This document contains six objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut Client Pro Objective

The TestOut Client Pro course covers the following TestOut Client Pro exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	
1.2	TestOut Lab Simulator	
1.3	Windows User Interface Overview	1.2 - Configure Windows settings 1.2.1 - Configure Windows desktop
1.4	Windows File and Folder Management	
2.0	**Windows Installation**	
2.1	Windows Versions	
2.2	Windows Installation	
2.3	Windows Activation	
2.4	Windows Post-Installation Configuration	
2.5	Printer and External Devices	4.1 - Configure and manage local printers 4.1.1 Add a printer

		4.1.2 Configure a default printer
2.6	Web Browser Configuration	1.1 - Configure Windows Internet settings 1.1.1 - Configure Internet Explorer cookie settings 1.1.2 - Configure the IE Popup Blocker
2.7	Windows Upgrade	
2.8	User Profile and Data Migration	
2.9	Windows Deployment	
3.0	**System Imaging**	
3.1	System Images	
3.2	Image Servicing	
3.3	Provisioning Packages	
3.4	Sideloaded Apps	
4.0	**Windows Device and User Management**	
4.1	Device and User Management	2.1 - Create and manage users and groups 2.1.1 - Create a local user account 2.1.2 - Create Active Directory (AD) user accounts 2.1.5 - Manage Active Directory (AD) user accounts
4.2	Active Directory	

4.3	Virtual Private Network (VPN)	3.1 - Configure network settings 3.1.1 - Configure and connect a virtual private network (VPN)
4.4	Secure Accounts and Certificates on Windows 10	
5.0	**Hardware Management**	
5.1	Devices and Drivers	4.3 - Configure and update device drivers 4.3.1 Configure driver updates 4.3.2 Roll back device drivers
5.2	Device Driver Troubleshooting	4.3 - Configure and update device drivers 4.3.2 Roll back device drivers
5.3	Display Management	
5.4	Local Storage	
5.5	OneDrive Storage	2.3 - Configure file permissions and encryption 2.3.4 - Configure offline files
6.0	**Network Configuration**	
6.1	IPv4	3.1 - Configure network settings 3.1.3 - Configure the static IP address
6.2	IPv6	

6.3	IP Configuration	3.1 - Configure network settings 3.1.2 - Configure IPv6 settings 3.1.3 - Configure the static IP address
6.4	IP Troubleshooting	3.3 - Troubleshoot networking 3.3.2 - Troubleshoot TCP/IP configuration
6.5	Wireless Networking Overview	
6.6	Wireless Networking Configuration	3.1 - Configure network settings 3.1.4 - Connect to a wireless network
7.0	**Application Management**	
7.1	Desktop Applications	
7.2	User Account Control	2.2 - Configure local policies 2.2.2 - Configure user account control (UAC) settings 2.2.3 - Set user account control (UAC) to defaults
7.3	Windows Store Apps	
7.4	Cloud-based Applications	
8.0	**System Access**	
8.1	Authentication and Authorization	
8.2	Authentication Management	2.1 - Create and manage users and groups 2.1.1 - Create a local user account

		2.1.2 - Create Active Directory (AD) user accounts 2.1.3 - Create and manage groups 2.1.4 - Manage user account types 2.1.5 - Manage Active Directory (AD) user accounts
8.3	User Rights and Account Policies	2.1 - Create and manage users and groups 2.1.1 - Create a local user account 2.1.2 - Create Active Directory (AD) user accounts 2.1.4 - Manage user account types 2.1.5 - Manage Active Directory (AD) user accounts 2.2 - Configure local policies 2.2.1 - Configure a password policy
8.4	Credential Management	
8.5	Alternative Authentication Options	1.2 - Configure Windows settings 1.2.3 - Create and configure an online account
8.6	NTFS Permissions	2.3 - Configure file permissions and encryption 2.3.3 - Configure NTFS file permissions
8.7	Auditing	
8.8	Dynamic Access Control (DAC)	
8.9	Encryption	2.3 - Configure file permissions and encryption 2.3.2 - Configure encryption
9.0	**Resource Sharing**	

9.1	File and Folder Sharing	2.3 - Configure file permissions and encryption 2.3.2 - Configure encryption 2.3.3 - Configure NTFS file permissions
9.2	Shared Resource Troubleshooting	
10.0	**Mobile Computing**	
10.1	Co-Management	
10.2	Mobile Device Management - Intune Enrollment	
10.3	Mobile Device Management - Intune Policies and Profiles	
10.4	BitLocker	2.3 - Configure file permissions and encryption 2.3.1 - Configure and start BitLocker 2.3.2 - Configure encryption
10.5	Mobile Device Security	2.4 - Configure and manage Windows Defender 2.4.4 - Configure Windows Security
10.6	Power Management	1.2 - Configure Windows settings 1.2.2 - Create a power plan
10.7	Mobility Options	1.1 - Configure Windows Internet settings 1.1.3 - Configure offline settings 2.3 - Configure file permissions and encryption

		2.3.4 - Configure offline files
10.8	Mobile Networking	3.1 - Configure network settings 3.1.4 - Connect to a wireless network
10.9	Mobile Apps	
10.10	Mobile Application Management with Intune	
11.0	**System Monitoring and Maintenance**	
11.1	System Configuration Tools	4.4 - Configure and start Window services 4.4.1 - Configure Windows services 4.4.2 - Start Windows services
11.2	System Events	
11.3	Performance Management	
11.4	Resource Monitoring	
11.5	Reliability and Performance Maintenance	
11.6	Windows Optimization	1.2 - Configure Windows settings 1.2.1 - Configure Windows desktop
11.7	Remote Management	3.2 - Enable and configure remote desktop 3.2.1 - Configure remote assistance

11.8	Remote Desktop and Remote Assistance	3.2 - Enable and configure remote desktop 3.2.1 - Configure remote assistance 3.2.2 - Enable remote desktop
11.9	System Troubleshooting Tools	4.4 - Configure and start Window services 4.4.2 - Start Windows services
12.0	**System Protection**	
12.1	Windows Updates	
12.2	Advanced Windows Updates	4.3 - Configure and update device drivers 4.3.1 Configure driver updates
12.3	System Restore	4.2 - Configure and perform file system backup and recovery 4.2.2 Create a Windows restore point
12.4	Backup	4.2 - Configure and perform file system backup and recovery 4.2.3 Enable and configure file history 4.2.4 Restore backup files
12.5	Recovery	4.2 - Configure and perform file system backup and recovery 4.2.3 Enable and configure file history 4.2.4 Restore backup files 4.2.5 Restore a previous version
12.6	Recovery Environment	

13.0	Threat Protection	
13.1	Malware Protection	2.4 - Configure and manage Windows Defender 2.4.4 - Configure Windows Security
13.2	Endpoint Security	2.4 - Configure and manage Windows Defender 2.4.4 - Configure Windows Security
13.3	Windows Defender Credential Guard	2.4 - Configure and manage Windows Defender 2.4.2 - Configure Windows Defender Credential Guard
13.4	Windows Defender Exploit Guard	2.4 - Configure and manage Windows Defender 2.4.3 - Configure Windows Defender Exploit Guard
13.5	Windows Defender Advanced Threat Protection	
13.6	Windows Defender Application Control	2.4 - Configure and manage Windows Defender 2.4.1 - Configure Windows Defender Application Control
13.7	Windows Defender Application Guard	
13.8	Windows Defender Firewall	2.4 - Configure and manage Windows Defender 2.4.5 - Enable and manage Windows Defender Firewall
13.9	Windows Defender Firewall with Advanced Security	2.4 - Configure and manage Windows Defender 2.4.5 - Enable and manage Windows Defender Firewall

Objective Mapping: TestOut Client Pro Objective to LabSim Section

The TestOut Client Pro course and certification exam cover the following TestOut Client Pro objectives:

#	Domain	Module.Section
1.0	**Configuration**	
1.1	Configure Windows Internet settings 1.1.1 - Configure Internet Explorer cookie settings 1.1.2 - Configure the IE Popup Blocker 1.1.3 - Configure offline settings	2.6 10.7
1.2	Configure Windows settings 1.2.1 - Configure Windows desktop 1.2.2 - Create a power plan 1.2.3 - Create and configure an online account	1.3 8.5 10.5, 10.6 11.6
2.0	**Management**	
2.1	Create and manage users and groups 2.1.1 - Create a local user account 2.1.2 - Create Active Directory (AD) user accounts 2.1.3 - Create and manage groups 2.1.4 - Manage user account types 2.1.5 - Manage Active Directory (AD) user accounts	4.1 8.2, 8.3

2.2	Configure local policies 2.2.1 - Configure a password policy 2.2.2 - Configure user account control (UAC) settings 2.2.3 - Set user account control (UAC) to defaults	7.2 8.3
2.3	Configure file permissions and encryption 2.3.1 - Configure and start BitLocker 2.3.2 - Configure encryption 2.3.3 - Configure NTFS file permissions 2.3.4 - Configure offline files	5.5 8.6, 8.9 9.1 10.4, 10.7
2.4	Configure and manage Windows Defender 2.4.1 - Configure Windows Defender Application Control 2.4.2 - Configure Windows Defender Credential Guard 2.4.3 - Configure Windows Defender Exploit Guard 2.4.4 - Configure Windows Security 2.4.5 - Enable and manage Windows Defender Firewall	10.5 13.1, 13.2, 13.3, 13.4, 13.6, 13.8, 13.9
3.0	**Networking**	
3.1	Configure network settings 3.1.1 - Configure and connect a virtual private network (VPN) 3.1.2 - Configure IPv6 settings 3.1.3 - Configure the static IP address 3.1.4 - Connect to a wireless network	4.3 6.1, 6.3, 6.6 10.8
3.2	Enable and configure remote desktop 3.2.1 - Configure remote assistance 3.2.2 - Enable remote desktop	11.7, 11.8

3.3	Troubleshoot networking 3.3.1 - Troubleshoot a network adapter 3.3.2 - Troubleshoot TCP/IP configuration	6.4
4.0	**Support**	
4.1	Configure and manage local printers 4.1.1 Add a printer 4.1.2 Configure a default printer	2.5
4.2	Configure and perform file system backup and recovery 4.2.1 Backup a computer 4.2.2 Create a Windows restore point 4.2.3 Enable and configure file history 4.2.4 Restore backup files 4.2.5 Restore a previous version	12.3, 12.4, 12.5
4.3	Configure and update device drivers 4.3.1 Configure driver updates 4.3.2 Roll back device drivers	5.1, 5.2 12.2
4.4	Configure and start Window services 4.4.1 - Configure Windows services 4.4.2 - Start Windows services	11.1, 11.9

Objective Mapping: LabSim Section to MD-100 Objective

The TestOut Client Pro course covers the following Microsoft MD-100: Windows 10 exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	
1.2	TestOut Lab Simulator	
1.3	Windows User Interface Overview	1.2 - Perform post-installation configuration 1.2.3 - Customize the Windows desktop
1.4	Windows File and Folder Management	
2.0	**Windows Installation**	
2.1	Windows Versions	1.1 - Install Windows 10 1.1.3 - Select the appropriate Windows edition
2.2	Windows Installation	1.1 - Install Windows 10 1.1.1 - Perform a clean installation
2.3	Windows Activation	1.2 - Perform post-installation configuration 1.2.4 - Troubleshoot activation issues

2.4	Windows Post-Installation Configuration	1.2 - Perform post-installation configuration 1.2.3 - Customize the Windows desktop 4.3 - Monitor and manage Windows 4.3.4 - Configure local registry
2.5	Printer and External Devices	1.2 - Perform post-installation configuration 1.2.5 - Configure printers and external devices
2.6	Web Browser Configuration	1.2 - Perform post-installation configuration 1.2.1 - Configure Edge and Internet Explorer
2.7	Windows Upgrade	1.1 - Install Windows 10 1.1.2 - Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.) 1.1.3 - Select the appropriate Windows edition
2.8	User Profile and Data Migration	
2.9	Windows Deployment	
3.0	**System Imaging**	
3.1	System Images	1.1 - Install Windows 10 1.1.2 - Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.)
3.2	Image Servicing	

3.3	Provisioning Packages	1.2 - Perform post-installation configuration 1.2.6 - Configure Windows 10 by using provisioning packages
3.4	Sideloaded Apps	
4.0	**Windows Device and User Management**	
4.1	Device and User Management	2.1 - Manage users, groups, and devices 2.1.1 - Manage local groups 2.1.2 - Manage local users 2.1.4 - Manage users, groups, and devices in Azure Active Directory 2.1.5 - Configure sign-in options
4.2	Active Directory	2.1 - Manage users, groups, and devices 2.1.1 - Manage local groups 2.1.2 - Manage local users 2.1.3 - Manage users, groups, and devices in Active Directory Domain Services 2.2 - Configure devices by using local policies 2.2.1 - Implement local policy 2.2.2 - Troubleshoot group policies on devices 2.2.3 - Configure Windows 10 settings by using group policy
4.3	Virtual Private Network (VPN)	
4.4	Secure Accounts and Certificates on Windows 10	
5.0	**Hardware Management**	
5.1	Devices and Drivers	

5.2	Device Driver Troubleshooting	
5.3	Display Management	4.3 - Monitor and manage Windows 4.3.3 - Manage Windows 10 environment
5.4	Local Storage	3.2 - Configure data access and protection 3.2.3 - Configure local storage 3.2.4 - Manage and optimize storage
5.5	OneDrive Storage	3.2 - Configure data access and protection 3.2.6 - Configure OneDrive/OneDrive for Business 4.1 - Configure system and data recovery 4.1.1 - Perform file recovery
6.0	**Network Configuration**	
6.1	IPv4	3.1 - Configure networking 3.1.1 - Configure client IP settings
6.2	IPv6	3.1 - Configure networking 3.1.1 - Configure client IP settings
6.3	IP Configuration	3.1 - Configure networking 3.1.1 - Configure client IP settings 3.1.2 - Configure mobile networking

6.4	IP Troubleshooting	3.1 - Configure networking 3.1.3 - Troubleshoot networking
6.5	Wireless Networking Overview	3.1 - Configure networking 3.1.2 - Configure mobile networking
6.6	Wireless Networking Configuration	3.1 - Configure networking 3.1.2 - Configure mobile networking 3.1.3 - Troubleshoot networking
7.0	**Application Management**	
7.1	Desktop Applications	1.2 - Perform post-installation configuration 1.2.8 - Configure application settings
7.2	User Account Control	2.3 - Manage Windows security 2.3.1 - Configure user account control (UAC)
7.3	Windows Store Apps	1.2 - Perform post-installation configuration 1.2.7 - Configure Microsoft Store settings
7.4	Cloud-based Applications	
8.0	**System Access**	
8.1	Authentication and Authorization	

8.2	Authentication Management	2.1 - Manage users, groups, and devices 2.1.1 - Manage local groups 2.1.2 - Manage local users
8.3	User Rights and Account Policies	2.1 - Manage users, groups, and devices 2.1.1 - Manage local groups 2.1.2 - Manage local users 2.1.3 - Manage users, groups, and devices in Active Directory Domain Services
8.4	Credential Management	
8.5	Alternative Authentication Options	2.1 - Manage users, groups, and devices 2.1.5 - Configure sign-in options
8.6	NTFS Permissions	3.2 - Configure data access and protection 3.2.1 - Configure NTFS permissions 3.2.2 - Configure shared permissions
8.7	Auditing	2.2 - Configure devices by using local policies 2.2.3 - Configure Windows 10 settings by using group policy 4.3 - Monitor and manage Windows 4.3.1 - Configure and analyze event logs
8.8	Dynamic Access Control (DAC)	3.2 - Configure data access and protection 3.2.1 - Configure NTFS permissions

8.9	Encryption	2.3 - Manage Windows security 2.3.3 - Implement encryption
9.0	**Resource Sharing**	
9.1	File and Folder Sharing	3.2 - Configure data access and protection 3.2.2 - Configure shared permissions 3.2.5 - Configure file and folder permissions
9.2	Shared Resource Troubleshooting	3.2 - Configure data access and protection 3.2.1 - Configure NTFS permissions 3.2.2 - Configure shared permissions 3.2.5 - Configure file and folder permissions
10.0	**Mobile Computing**	
10.1	Co-Management	
10.2	Mobile Device Management - Intune Enrollment	
10.3	Mobile Device Management - Intune Policies and Profiles	
10.4	BitLocker	2.3 - Manage Windows security 2.3.3 - Implement encryption
10.5	Mobile Device Security	
10.6	Power Management	1.2 - Perform post-installation configuration

		1.2.2 - Configure mobility settings
10.7	Mobility Options	1.2 - Perform post-installation configuration 1.2.2 - Configure mobility settings
10.8	Mobile Networking	3.1 - Configure networking 3.1.2 - Configure mobile networking
10.9	Mobile Apps	2.1 - Manage users, groups, and devices 2.1.4 - Manage users, groups, and devices in Azure Active Directory
10.10	Mobile Application Management with Intune	
11.0	**System Monitoring and Maintenance**	
11.1	System Configuration Tools	1.2 - Perform post-installation configuration 1.2.9 - Configure and manage services 4.3 - Monitor and manage Windows 4.3.5 - Schedule Tasks
11.2	System Events	4.3 - Monitor and manage Windows 4.3.1 - Configure and analyze event logs
11.3	Performance Management	4.3 - Monitor and manage Windows 4.3.2 - Manage performance

11.4	Resource Monitoring	4.3 - Monitor and manage Windows 4.3.2 - Manage performance
11.5	Reliability and Performance Maintenance	4.3 - Monitor and manage Windows 4.3.2 - Manage performance 4.3.3 - Manage Windows 10 environment
11.6	Windows Optimization	4.3 - Monitor and manage Windows 4.3.3 - Manage Windows 10 environment
11.7	Remote Management	4.4 - Configure remote connectivity 4.4.1 - Manage Windows 10 remotely by using Windows Admin Center 4.4.2 - Configure remote assistance tools including Remote Assist and Quick Assist 4.4.3 - Manage Windows remotely by using Windows Remote Management and PS remoting 4.4.4 - Configure remote desktop access
11.8	Remote Desktop and Remote Assistance	4.4 - Configure remote connectivity 4.4.2 - Configure remote assistance tools including Remote Assist and Quick Assist 4.4.4 - Configure remote desktop access
11.9	System Troubleshooting Tools	4.1 - Configure system and data recovery 4.1.3 - Troubleshoot startup/boot process 4.3 - Monitor and manage Windows 4.3.1 - Configure and analyze event logs

		4.3.2 - Manage performance 4.4 - Configure remote connectivity 4.4.3 - Manage Windows remotely by using Windows Remote Management and PS remoting
12.0	**System Protection**	
12.1	Windows Updates	1.2 - Perform post-installation configuration 1.2.7 - Configure Microsoft Store settings 4.2 - Manage updates 4.2.1 - Troubleshoot updates 4.2.2 - Select the appropriate servicing channel 4.2.3 - Configure Windows update options 4.2.4 - Plan for Windows updates
12.2	Advanced Windows Updates	4.2 - Manage updates 4.2.1 - Troubleshoot updates 4.2.3 - Configure Windows update options 4.2.5 - Configure updates by using Windows Update for Business
12.3	System Restore	4.1 - Configure system and data recovery 4.1.2 - Recover Windows 10 4.1.4 - Create and manage system restore points
12.4	Backup	4.1 - Configure system and data recovery 4.1.1 - Perform file recovery 4.1.2 - Recover Windows 10

12.5	Recovery	4.1 - Configure system and data recovery 4.1.1 - Perform file recovery
12.6	Recovery Environment	4.1 - Configure system and data recovery 4.1.2 - Recover Windows 10 4.1.3 - Troubleshoot startup/boot process
13.0	**Threat Protection**	
13.1	Malware Protection	
13.2	Endpoint Security	2.3 - Manage Windows security 2.3.2 - Configure Windows Defender Firewall 2.3.4 - Configure Windows Defender Antivirus
13.3	Windows Defender Credential Guard	
13.4	Windows Defender Exploit Guard	
13.5	Windows Defender Advanced Threat Protection	
13.6	Windows Defender Application Control	
13.7	Windows Defender Application Guard	
13.8	Windows Defender Firewall	2.3 - Manage Windows security 2.3.2 - Configure Windows Defender Firewall

13.9	Windows Defender Firewall with Advanced Security	2.3 - Manage Windows security 2.3.2 - Configure Windows Defender Firewall

Objective Mapping: MD-100 Objective to LabSim Section

The TestOut Client Pro course and certification exam cover the following Microsoft MD-100: Windows 10 objectives:

#	Domain	Module.Section
1.0	**Deploy Windows**	
1.1	Install Windows 10 1.1.1 - Perform a clean installation 1.1.2 - Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.) 1.1.3 - Select the appropriate Windows edition	2.1, 2.2, 2.7 3.1
1.2	Perform post-installation configuration 1.2.1 - Configure Edge and Internet Explorer 1.2.2 - Configure mobility settings 1.2.3 - Customize the Windows desktop 1.2.4 - Troubleshoot activation issues 1.2.5 - Configure printers and external devices 1.2.6 - Configure Windows 10 by using provisioning packages 1.2.7 - Configure Microsoft Store settings 1.2.8 - Configure application settings 1.2.9 - Configure and manage services	1.3 2.3, 2.4, 2.5, 2.6 3.3 7.1, 7.3 10.6, 10.7 11.1 12.1
2.0	**Manage devices and data**	
2.1	Manage users, groups, and devices 2.1.1 - Manage local groups 2.1.2 - Manage local users 2.1.3 - Manage users, groups, and devices in Active Directory Domain Services 2.1.4 - Manage users, groups, and devices in Azure Active Directory 2.1.5 - Configure sign-in options	4.1, 4.2 8.2, 8.3, 8.5 10.9

2.2	Configure devices by using local policies 2.2.1 - Implement local policy 2.2.2 - Troubleshoot group policies on devices 2.2.3 - Configure Windows 10 settings by using group policy	4.2 8.7
2.3	Manage Windows security 2.3.1 - Configure user account control (UAC) 2.3.2 - Configure Windows Defender Firewall 2.3.3 - Implement encryption 2.3.4 - Configure Windows Defender Antivirus	7.2 8.9 10.4 13.2, 13.8, 13.9
3.0	**Configure storage and connectivity**	
3.1	- Configure networking 3.1.1 - Configure client IP settings 3.1.2 - Configure mobile networking 3.1.3 - Troubleshoot networking	6.1, 6.2, 6.3, 6.4, 6.5, 6.6 10.8
3.2	- Configure data access and protection 3.2.1 - Configure NTFS permissions 3.2.2 - Configure shared permissions 3.2.3 - Configure local storage 3.2.4 - Manage and optimize storage 3.2.5 - Configure file and folder permissions 3.2.6 - Configure OneDrive/OneDrive for Business	5.4, 5.5 8.6, 8.8 9.1, 9.2
4.0	**Maintain Windows**	
4.1	Configure system and data recovery 4.1.1 - Perform file recovery 4.1.2 - Recover Windows 10 4.1.3 - Troubleshoot startup/boot process	5.5 11.9 12.3, 12.4, 12.5, 12.6

	4.1.4 - Create and manage system restore points	
4.2	Manage updates 4.2.1 - Troubleshoot updates 4.2.2 - Select the appropriate servicing channel 4.2.3 - Configure Windows update options 4.2.4 - Plan for Windows updates 4.2.5 - Configure updates by using Windows Update for Business	12.1, 12.2
4.3	Monitor and manage Windows 4.3.1 - Configure and analyze event logs 4.3.2 - Manage performance 4.3.3 - Manage Windows 10 environment 4.3.4 - Configure local registry 4.3.5 - Schedule Tasks	2.4 5.3 8.7 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.9
4.4	Configure remote connectivity 4.4.1 - Manage Windows 10 remotely by using Windows Admin Center 4.4.2 - Configure remote assistance tools including Remote Assist and Quick Assist 4.4.3 - Manage Windows remotely by using Windows Remote Management and PS remoting 4.4.4 - Configure remote desktop access	11.7, 11.8, 11.9

Objective Mapping: LabSim Section to MD-101 Objective

The TestOut Client Pro course covers the following Microsoft MD-101: Managing Modern Desktops exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	
1.2	TestOut Lab Simulator	
1.3	Windows User Interface Overview	
1.4	Windows File and Folder Management	
2.0	**Windows Installation**	
2.1	Windows Versions	
2.2	Windows Installation	
2.3	Windows Activation	
2.4	Windows Post-Installation Configuration	
2.5	Printer and External Devices	
2.6	Web Browser Configuration	
2.7	Windows Upgrade	1.1 - Plan a Windows 10 deployment 1.1.1 - Assess infrastructure readiness 1.1.3 - Plan upgrade and downgrade paths

		1.1.4 - Plan app compatibility
2.8	User Profile and Data Migration	1.1 - Plan a Windows 10 deployment 1.1.5 - Plan for user state
2.9	Windows Deployment	1.1 - Plan a Windows 10 deployment 1.1.2 - Evaluate and select appropriate deployment options (Endpoint Manager, MDT) 1.2 - Plan and implement Windows 10 by using Windows Autopilot 1.2.1 - Choose method based on requirements 1.2.2 - Create, validate, and assign deployment profile 1.2.3 - Extract device HW information to CSV file 1.2.4 - Import device HW information to cloud service 1.2.5 - Deploy Windows 10 1.2.6 - Troubleshoot deployment
3.0	**System Imaging**	
3.1	System Images	1.3 - Plan and implement Windows 10 using MDT 1.3.1 - Choose configuration options based on requirements 1.3.2 - Create and manage images 1.3.3 - Deploy images (may include WDS) 1.3.4 - Create and use task sequences 1.3.5 - Manage application and driver deployment 1.3.6 - Monitor and troubleshoot deployment
3.2	Image Servicing	
3.3	Provisioning Packages	

3.4	Sideloaded Apps	4.1 - Deploy and update applications 4.1.5 - Enable sideloading of apps into images
4.0	**Windows Device and User Management**	
4.1	Device and User Management	
4.2	Active Directory	
4.3	Virtual Private Network (VPN)	1.4 - Manage accounts, VPN connections, and certificates on Windows 10 1.4.2 - Configure VPN client
4.4	Secure Accounts and Certificates on Windows 10	1.4 - Manage accounts, VPN connections, and certificates on Windows 10 1.4.1 - Secure privileged accounts on Windows 10 1.4.3 - Configure and manage certificates on client devices
5.0	**Hardware Management**	
5.1	Devices and Drivers	
5.2	Device Driver Troubleshooting	
5.3	Display Management	
5.4	Local Storage	
5.5	OneDrive Storage	
6.0	**Network Configuration**	
6.1	IPv4	

6.2	IPv6	
6.3	IP Configuration	
6.4	IP Troubleshooting	
6.5	Wireless Networking Overview	
6.6	Wireless Networking Configuration	
7.0	**Application Management**	
7.1	Desktop Applications	
7.2	User Account Control	
7.3	Windows Store Apps	4.1 - Deploy and update applications 4.1.3 - Deploy apps by using Microsoft Store for Business/iTunes/Google Play
7.4	Cloud-based Applications	4.1 - Deploy and update applications 4.1.4 - Deploy Microsoft 365 Apps for enterprise using Microsoft Intune 4.1.6 - Gather Microsoft 365 Apps readiness data
8.0	**System Access**	
8.1	Authentication and Authorization	
8.2	Authentication Management	
8.3	User Rights and Account Policies	

8.4	Credential Management	
8.5	Alternative Authentication Options	2.3 - Manage user profiles 2.3.3 - Configure sync settings
8.6	NTFS Permissions	
8.7	Auditing	
8.8	Dynamic Access Control (DAC)	
8.9	Encryption	
9.0	**Resource Sharing**	
9.1	File and Folder Sharing	
9.2	Shared Resource Troubleshooting	
10.0	**Mobile Computing**	
10.1	Co-Management	
10.2	Mobile Device Management - Intune Enrollment	2.1 - Implement compliance policies for devices 2.1.1 - Implement device compliance policies 2.1.2 - Manage device compliance policies 2.1.3 - Plan device compliance policies 3.2 - Manage Microsoft Intune devices 3.2.1 - Configure enrollment settings in Microsoft Intune 3.2.2 - Configure Microsoft Intune automatic and bulk enrollment 3.2.3 - Enroll non-Windows devices

		3.2.4 - Enroll Windows devices
10.3	Mobile Device Management - Intune Policies and Profiles	2.1 - Implement compliance policies for devices 2.1.1 - Implement device compliance policies 2.1.2 - Manage device compliance policies 2.1.3 - Plan device compliance policies 2.2 - Configure device profiles 2.2.1 - Implement device profiles; Manage device profiles 2.2.2 - Plan device profiles, Control policy conflicts 2.2.3 - Configure and implement assigned access or public devices 2.3 - Manage user profiles 2.3.1 - Configure user profiles 2.3.2 - Configure Enterprise State Roaming in Azure AD 3.2 - Manage Microsoft Intune devices 3.2.5 - Review device inventory
10.4	BitLocker	
10.5	Mobile Device Security	3.3 - Monitor devices 3.3.1 - Monitor devices using Azure Monitor and Desktop Analytics 3.3.2 - Monitor device inventory reports using Endpoint Manger Admin Center
10.6	Power Management	
10.7	Mobility Options	
10.8	Mobile Networking	

10.9	Mobile Apps	2.2 - Configure device profiles 2.2.3 - Configure and implement assigned access or public devices 4.1 - Deploy and update applications 4.1.1 - Assign apps to groups 4.1.2 - Deploy apps by using Microsoft Intune
10.10	Mobile Application Management with Intune	4.1 - Deploy and update applications 4.1.1 - Assign apps to groups 4.1.2 - Deploy apps by using Microsoft Intune 4.2 - Implement Mobile Application Management (MAM) 4.2.1 - Implement App Protection policies 4.2.2 - Manage App Protection policies 4.2.3 - Plan App Protection Policies 4.2.4 - Plan and implement App Configuration Policies (Windows Information Protection)
11.0	**System Monitoring and Maintenance**	
11.1	System Configuration Tools	
11.2	System Events	
11.3	Performance Management	
11.4	Resource Monitoring	
11.5	Reliability and Performance Maintenance	
11.6	Windows Optimization	

11.7	Remote Management	
11.8	Remote Desktop and Remote Assistance	
11.9	System Troubleshooting Tools	3.3 - Monitor devices 3.3.1 - Monitor devices using Azure Monitor and Desktop Analytics 3.3.2 - Monitor device inventory reports using Endpoint Manger Admin Center
12.0	**System Protection**	
12.1	Windows Updates	3.4 - Manage updates 3.4.1 - Configure Windows 10 delivery optimization 3.4.2 - Deploy Windows updates using Microsoft Intune 3.4.3 - Monitor Windows 10 updates
12.2	Advanced Windows Updates	3.4 - Manage updates 3.4.1 - Configure Windows 10 delivery optimization 3.4.2 - Deploy Windows updates using Microsoft Intune 3.4.3 - Monitor Windows 10 updates
12.3	System Restore	
12.4	Backup	
12.5	Recovery	
12.6	Recovery Environment	
13.0	**Threat Protection**	
13.1	Malware Protection	

13.2	Endpoint Security	**3.1 - Manage Windows Defender** 3.1.6 - Protect devices using Endpoint Security 3.1.7 - Manage enterprise-level disk encryption 3.1.8 - Implement and manage security baselines in Microsoft Intune
13.3	Windows Defender Credential Guard	**3.1 - Manage Windows Defender** 3.1.2 - Implement and manage Windows Defender Credential Guard
13.4	Windows Defender Exploit Guard	**3.1 - Manage Windows Defender** 3.1.3 - Implement and manage Windows Defender Exploit Guard
13.5	Windows Defender Advanced Threat Protection	**3.1 - Manage Windows Defender** 3.1.4 - Plan and Implement Microsoft Defender Advanced Threat Protection for Windows 10
13.6	Windows Defender Application Control	**3.1 - Manage Windows Defender** 3.1.5 - Integrate Windows Defender Application Control
13.7	Windows Defender Application Guard	**3.1 - Manage Windows Defender** 3.1.1 - Implement and manage Windows Defender Application Guard
13.8	Windows Defender Firewall	
13.9	Windows Defender Firewall with Advanced Security	

Objective Mapping: MD-101 Objective to LabSim Section

The TestOut Client Pro course and certification exam cover the following Microsoft MD-101: Managing Modern Desktops objectives:

#	Domain	Module.Section
1.0	Plan a Windows Deployment	
1.1	Plan a Windows 10 deployment 1.1.1 - Assess infrastructure readiness 1.1.2 - Evaluate and select appropriate deployment options (Endpoint Manager, MDT) 1.1.3 - Plan upgrade and downgrade paths 1.1.4 - Plan app compatibility 1.1.5 - Plan for user state	2.7, 2.8, 2.9
1.2	Plan and implement Windows 10 by using Windows Autopilot 1.2.1 - Choose method based on requirements 1.2.2 - Create, validate, and assign deployment profile 1.2.3 - Extract device HW information to CSV file 1.2.4 - Import device HW information to cloud service 1.2.5 - Deploy Windows 10 1.2.6 - Troubleshoot deployment	2.9
1.3	Plan and implement Windows 10 using MDT 1.3.1 - Choose configuration options based on requirements 1.3.2 - Create and manage images 1.3.3 - Deploy images (may include WDS) 1.3.4 - Create and use task sequences 1.3.5 - Manage application and driver deployment 1.3.6 - Monitor and troubleshoot deployment	3.1
1.4	Manage accounts, VPN connections, and certificates on Windows 10	4.3, 4.4

	1.4.1 - Secure privileged accounts on Windows 10 1.4.2 - Configure VPN client 1.4.3 - Configure and manage certificates on client devices	
2.0	**Manage policies and profiles**	
2.1	Implement compliance policies for devices 2.1.1 - Implement device compliance policies 2.1.2 - Manage device compliance policies 2.1.3 - Plan device compliance policies	10.2, 10.3
2.2	Configure device profiles 2.2.1 - Implement device profiles; Manage device profiles 2.2.2 - Plan device profiles, Control policy conflicts 2.2.3 - Configure and implement assigned access or public devices	10.3, 10.9
2.3	Manage user profiles 2.3.1 - Configure user profiles 2.3.2 - Configure Enterprise State Roaming in Azure AD 2.3.3 - Configure sync settings	8.5 10.3
3.0	**Manage and protect devices**	
3.1	Manage Windows Defender 3.1.1 - Implement and manage Windows Defender Application Guard 3.1.2 - Implement and manage Windows Defender Credential Guard 3.1.3 - Implement and manage Windows Defender Exploit Guard 3.1.4 - Plan and Implement Microsoft Defender Advanced Threat Protection for Windows 10 3.1.5 - Integrate Windows Defender Application Control 3.1.6 - Protect devices using Endpoint Security 3.1.7 - Manage enterprise-level disk encryption	13.2, 13.3, 13.4, 13.5, 13.6, 13.7

	3.1.8 - Implement and manage security baselines in Microsoft Intune	
3.2	Manage Microsoft Intune devices 3.2.1 - Configure enrollment settings in Microsoft Intune 3.2.2 - Configure Microsoft Intune automatic and bulk enrollment 3.2.3 - Enroll non-Windows devices 3.2.4 - Enroll Windows devices 3.2.5 - Review device inventory	10.2, 10.3
3.3	Monitor devices 3.3.1 - Monitor devices using Azure Monitor and Desktop Analytics 3.3.2 - Monitor device inventory reports using Endpoint Manger Admin Center	10.5 11.9
3.4	Manage updates 3.4.1 - Configure Windows 10 delivery optimization 3.4.2 - Deploy Windows updates using Microsoft Intune 3.4.3 - Monitor Windows 10 updates	12.1, 12.2
4.0	**Manage apps and data**	
4.1	Deploy and update applications 4.1.1 - Assign apps to groups 4.1.2 - Deploy apps by using Microsoft Intune 4.1.3 - Deploy apps by using Microsoft Store for Business/iTunes/Google Play 4.1.4 - Deploy Microsoft 365 Apps for enterprise using Microsoft Intune 4.1.5 - Enable sideloading of apps into images 4.1.6 - Gather Microsoft 365 Apps readiness data	3.4 7.3, 7.4 10.9, 10.10
4.2	Implement Mobile Application Management (MAM) 4.2.1 - Implement App Protection policies 4.2.2 - Manage App Protection policies	10.10

	4.2.3 - Plan App Protection Policies 4.2.4 - Plan and implement App Configuration Policies (Windows Information Protection)	