TestOut

TestOut Client Pro – English 6.0.x

Objective Mappings:

TestOut Client Pro
Microsoft MD-100
Microsoft MD-101

Powered by LABSIM

Contents

This document contains four 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	2.3 Configure file permissions and encryption 2.3.3 Configure NTFS file permissions 2.3.4 Configure offline files
2.0	**Windows Installation**	
2.1	Windows Versions	
2.2	Windows Installation	
2.3	Windows Activation	
2.4	Windows Post-Installation Configuration	
2.5	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
2.6	Windows Upgrade	
2.7	User Profile and Data Migration	
2.8	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	
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	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 (UAC)	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	2.4 Configure and manage Windows Defender
		2.4.2 Configure Windows Defender Credential Guard
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	Resource 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	
9.3	Printer Management and Sharing	4.1 Configure and manage local printers
		4.1.1 Add a printer

		4.1.2 Configure a default printer
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	Virtual Private Network (VPN)	3.1 Configure network settings 3.1.1 Configure and connect a virtual private network (VPN)
10.5	BitLocker	2.3 Configure file permissions and encryption 2.3.1 Configure and start BitLocker 2.3.2 Configure encryption
10.6	Mobile Device Security	2.4 Configure and manage Windows Defender 2.4.4 Configure Windows Security
10.7	Power Management	1.2 Configure Windows settings 1.2.2 Create a power plan
10.8	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

10.9	Mobile Networking	3.1 Configure network settings 3.1.4 Connect to a wireless network
10.10	Mobile Apps	
10.11	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	**Windows Defender**	

13.1	Malware Protection	2.4 Configure and manage Windows Defender 2.4.4 Configure Windows Security
13.2	Windows 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	2.5 10.8
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 10.6, 10.7 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	7.2 8.3

		2.2.3 Set user account control (UAC) to defaults	
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	1.4 5.4 8.6, 8.9 9.1 10.5, 10.8
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	8.4 10.6 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	6.1, 6.3, 6.6 10.4, 10.9
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	6.4

		3.3.2 Troubleshoot TCP/IP configuration	
4.0	**Support**		
4.1	Configure and manage local printers 4.1.1 Add a printer 4.1.2 Configure a default printer		9.3
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 1.2.4 Customize the Windows desktop
1.4	Windows File and Folder Management	2.2 Configure data access and protection 2.2.1 Configure NTFS permissions 2.2.2 Configure shared permissions
2.0	**Windows Installation**	
2.1	Windows Versions	1.1 Deploy Windows 10 1.1.5 Select the appropriate Windows edition
2.2	Windows Installation	1.1 Deploy Windows 10 1.1.2 Perform a clean installation
2.3	Windows Activation	1.1 Deploy Windows 10

		1.1.6 Troubleshoot activation issues

2.4	Windows Post-Installation Configuration	1.1 Deploy Windows 10
		
		    1.1.1 Configure language packs
		
		1.2 Perform post-installation configuration
		
		    1.2.1 Configure Edge and Internet Explorer
		    1.2.3 Configure sign-in options
		    1.2.4 Customize the Windows desktop
		
		2.3 Configure devices by using local policies
		
		    2.3.1 Configure local registry

2.5	Web Browser Configuration	1.2 Perform post-installation configuration 1.2.1 Configure Edge and Internet Explorer
2.6	Windows Upgrade	1.1 Deploy Windows 10 1.1.4 Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.)
2.7	User Profile and Data Migration	1.1 Deploy Windows 10 1.1.3 Migrate user data
2.8	Windows Deployment	
3.0	**System Imaging**	
3.1	System Images	1.1 Deploy Windows 10

			1.1.2 Perform a clean installation 1.1.4 Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.)
3.2	Image Servicing		1.1 Deploy Windows 10 1.1.2 Perform a clean installation
3.3	Provisioning Packages		
3.4	Sideloaded Apps		
4.0	**Windows Device and User Management**		
4.1	Device and User Management		2.1 Manage local users, local groups, and devices 2.1.3 Manage local users
4.2	Active Directory		2.1 Manage local users, local groups, and devices 2.1.1 Manage devices in directories 2.3 Configure devices by using local policies 2.3.2 Implement local policy 2.3.3 Troubleshoot group policies on devices
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	OneDrive Storage	**4.1 Configure system and data recovery** 4.1.1 Perform file recovery (including OneDrive)
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
6.4	IP Troubleshooting	**3.1 Configure networking** 3.1.4 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 3.1.4 Troubleshoot networking 3.1.5 Configure Wi-Fi profiles

7.0	**Application Management**	
7.1	Desktop Applications	4.3 Monitor and manage Windows 4.3.3 Manage Windows 10 environment
7.2	User Account Control (UAC)	2.4 Manage Windows security 2.4.1 Configure user account control (UAC)
7.3	Windows Store Apps	
7.4	Cloud-based Applications	
8.0	**System Access**	
8.1	Authentication and Authorization	2.2 Configure data access and protection 2.2.1 Configure NTFS permissions
8.2	Authentication Management	2.1 Manage local users, local groups, and devices 2.1.2 Manage local groups 2.1.3 Manage local users
8.3	User Rights and Account Policies	2.1 Manage local users, local groups, and devices 2.1.3 Manage local users
8.4	Credential Management	
8.5	Alternative Authentication Options	1.2 Perform post-installation configuration

		1.2.3 Configure sign-in options
8.6	NTFS Permissions	2.2 Configure data access and protection 2.2.1 Configure NTFS permissions
8.7	Auditing	4.3 Monitor and manage Windows 4.3.1 Configure and analyze event logs
8.8	Dynamic Access Control (DAC)	2.2 Configure data access and protection 2.2.1 Configure NTFS permissions
8.9	Encryption	2.4 Manage Windows security 2.4.3 Implement encryption
9.0	**Resource Sharing**	
9.1	Resource Sharing	2.2 Configure data access and protection 2.2.2 Configure shared permissions
9.2	Shared Resource Troubleshooting	2.2 Configure data access and protection 2.2.1 Configure NTFS permissions 2.2.2 Configure shared permissions
9.3	Printer Management and Sharing	
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	Virtual Private Network (VPN)	3.1 Configure networking 3.1.3 Configure VPN client
10.5	BitLocker	2.4 Manage Windows security 2.4.3 Implement encryption
10.6	Mobile Device Security	
10.7	Power Management	1.2 Perform post-installation configuration 1.2.2 Configure mobility settings
10.8	Mobility Options	1.2 Perform post-installation configuration 1.2.2 Configure mobility settings
10.9	Mobile Networking	3.1 Configure networking 3.1.2 Configure mobile networking 3.1.5 Configure Wi-Fi profiles
10.10	Mobile Apps	
10.11	Mobile Application Management with Intune	

11.0	System Monitoring and Maintenance	
11.1	System Configuration Tools	4.1 Configure system and data recovery 4.1.3 Troubleshoot startup/boot process
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	3.2 Configure remote connectivity 3.2.1 Configure remote management 3.2.2 Enable PowerShell Remoting 3.2.3 Configure remote desktop access

11.8	Remote Desktop and Remote Assistance	**3.2 Configure remote connectivity** 3.2.1 Configure remote management 3.2.3 Configure remote desktop access
11.9	System Troubleshooting Tools	**3.2 Configure remote connectivity** 3.2.2 Enable PowerShell Remoting **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 4.3.3 Manage Windows 10 environment
12.0	**System Protection**	
12.1	Windows Updates	**4.2 Manage updates** 4.2.1 Check for updates 4.2.2 Troubleshoot updates 4.2.3 Validate and test updates 4.2.4 Select the appropriate servicing channel 4.2.5 Configure Windows update options
12.2	Advanced Windows Updates	**4.2 Manage updates** 4.2.2 Troubleshoot updates 4.2.3 Validate and test updates 4.2.5 Configure Windows update options
12.3	System Restore	**4.1 Configure system and data recovery**

		4.1.2 Recover Windows 10	
12.4	Backup	**4.1 Configure system and data recovery**	
		4.1.1 Perform file recovery (including OneDrive) 4.1.2 Recover Windows 10	
12.5	Recovery	**4.1 Configure system and data recovery**	
		4.1.1 Perform file recovery (including OneDrive)	
12.6	Recovery Environment	**1.1 Deploy Windows 10**	
		1.1.2 Perform a clean installation	
		4.1 Configure system and data recovery	
		4.1.2 Recover Windows 10 4.1.3 Troubleshoot startup/boot process	
13.0	**Windows Defender**		
13.1	Malware Protection		
13.2	Windows Security	**2.4 Manage Windows security**	
		2.4.2 Configure Windows Defender Firewall	
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	2.4 Manage Windows security 2.4.2 Configure Windows Defender Firewall
13.9	Windows Defender Firewall with Advanced Security	2.4 Manage Windows security 2.4.2 Configure Windows Defender Firewall

Objective Mapping: MD-100 Objective to LabSim Section

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

#	Domain	Module.Section
1.0	**Deploy Windows**	
1.1	Deploy Windows 10 1.1.1 Configure language packs 1.1.2 Perform a clean installation 1.1.3 Migrate user data 1.1.4 Perform an in-place upgrade (using tools such as MDT, WDS, ADK, etc.) 1.1.5 Select the appropriate Windows edition 1.1.6 Troubleshoot activation issues	2.1, 2.2, 2.3, 2.4, 2.6, 2.7 3.1, 3.2 12.6
1.2	Perform post-installation configuration 1.2.1 Configure Edge and Internet Explorer	1.3 2.4, 2.5

		1.2.2 Configure mobility settings 1.2.3 Configure sign-in options 1.2.4 Customize the Windows desktop	8.5 10.7, 10.8
2.0	**Manage devices and data**		
2.1	Manage local users, local groups, and devices 2.1.1 Manage devices in directories 2.1.2 Manage local groups 2.1.3 Manage local users		4.1, 4.2 8.2, 8.3
2.2	Configure data access and protection 2.2.1 Configure NTFS permissions 2.2.2 Configure shared permissions		1.4 8.1, 8.6, 8.8 9.1, 9.2
2.3	Configure devices by using local policies 2.3.1 Configure local registry 2.3.2 Implement local policy 2.3.3 Troubleshoot group policies on devices		2.4 4.2
2.4	Manage Windows security 2.4.1 Configure user account control (UAC) 2.4.2 Configure Windows Defender Firewall 2.4.3 Implement encryption		7.2 8.9 10.5 13.2, 13.8, 13.9
3.0	**Configure connectivity**		
3.1	Configure networking 3.1.1 Configure client IP settings 3.1.2 Configure mobile networking 3.1.3 Configure VPN client		6.1, 6.2, 6.3, 6.4, 6.5, 6.6 10.4, 10.9

		3.1.4 Troubleshoot networking 3.1.5 Configure Wi-Fi profiles	
	3.2	Configure remote connectivity 3.2.1 Configure remote management 3.2.2 Enable PowerShell Remoting 3.2.3 Configure remote desktop access	11.7, 11.8, 11.9
4.0	**Maintain Windows**		
	4.1	Configure system and data recovery 4.1.1 Perform file recovery (including OneDrive) 4.1.2 Recover Windows 10 4.1.3 Troubleshoot startup/boot process	5.4 11.1, 11.9 12.3, 12.4, 12.5, 12.6
	4.2	Manage updates 4.2.1 Check for updates 4.2.2 Troubleshoot updates 4.2.3 Validate and test updates 4.2.4 Select the appropriate servicing channel 4.2.5 Configure Windows update options	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	5.3 7.1 8.7 11.2, 11.3, 11.4, 11.5, 11.6, 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	Web Browser Configuration	4.1 Deploy and update applications 4.1.7 Configure IE Enterprise mode
2.6	Windows Upgrade	1.3 Upgrade devices to Windows 10 1.3.1 Identify upgrade and downgrade paths 1.3.2 Manage in-place upgrades 1.3.3 Configure a Windows analytics environment

		1.3.4 Perform Upgrade Readiness assessment
2.7	User Profile and Data Migration	**1.3 Upgrade devices to Windows 10** 1.3.5 Migrate user profiles
2.8	Windows Deployment	**1.1 Plan and implement Windows 10 by using dynamic deployment** 1.1.1 Evaluate and select an appropriate deployment option 1.1.2 Pilot deployment **1.2 Plan and implement Windows 10 by using Windows Autopilot** 1.2.1 Evaluate and select an appropriate deployment option 1.2.2 Pilot deployment 1.2.3 Create, validate, and assign deployment profile 1.2.4 Extract device HW information to CSV file 1.2.5 Import device HW information to cloud service 1.2.6 Troubleshoot deployment
3.0	**System Imaging**	
3.1	System Images	**1.1 Plan and implement Windows 10 by using dynamic deployment** 1.1.1 Evaluate and select an appropriate deployment option 1.1.2 Pilot deployment
3.2	Image Servicing	
3.3	Provisioning Packages	**1.1 Plan and implement Windows 10 by using dynamic deployment** 1.1.3 Manage and troubleshoot 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	**1.5 Manage device authentication** 1.5.3 Perform Azure AD join
4.2	Active Directory	
5.0	**Hardware Management**	
5.1	Devices and Drivers	
5.2	Device Driver Troubleshooting	
5.3	Display Management	
5.4	OneDrive Storage	**2.4 Manage user profiles** 2.4.4 Implement Folder Redirection (including OneDrive)
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 (UAC)	
7.3	Windows Store Apps	4.1 Deploy and update applications 4.1.3 Deploy apps by using Microsoft Store for Business
7.4	Cloud-based Applications	4.1 Deploy and update applications 4.1.4 Deploy O365 ProPlus 4.1.6 Gather Office 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	3.1 Manage Windows Defender 3.1.2 Implement and manage Windows Defender Credential Guard
8.5	Alternative Authentication Options	1.5 Manage device authentication 1.5.2 Manage sign-on options
8.6	NTFS Permissions	

8.7	Auditing	
8.8	Dynamic Access Control (DAC)	
8.9	Encryption	
9.0	**Resource Sharing**	
9.1	Resource Sharing	
9.2	Shared Resource Troubleshooting	
9.3	Printer Management and Sharing	
10.0	**Mobile Computing**	
10.1	Co-Management	2.1 Plan and implement co-management 2.1.1 Implement co-management precedence 2.1.2 Migrate group policy to MDM policies 2.1.3 recommend a co-management strategy
10.2	Mobile Device Management - Intune Enrollment	2.2 Implement conditional access and compliance policies for devices 2.2.1 Implement conditional access policies 2.2.2 Manage conditional access policies 2.2.3 plan conditional access policies 2.2.4 Implement device compliance policies 2.2.5 Manage device compliance policies 2.2.6 plan device compliance policies 3.2 Manage Intune device enrollment and inventory 3.2.1 Configure enrollment settings 3.2.2 Configure Intune automatic enrollment 3.2.3 Enable device enrollment 3.2.4 Enroll non-Windows devices

		3.2.5 Enroll Windows devices 3.2.6 Generate custom device inventory reports	
10.3	Mobile Device Management - Intune Policies and Profiles	**1.5 Manage device authentication** 1.5.1 Manage authentication policies **2.2 Implement conditional access and compliance policies for devices** 2.2.1 Implement conditional access policies 2.2.2 Manage conditional access policies 2.2.4 Implement device compliance policies 2.2.5 Manage device compliance policies 2.2.6 plan device compliance policies **2.3 Configure device profiles** 2.3.1 Implement device profiles 2.3.2 Manage device profiles 2.3.3 plan device profiles **2.4 Manage user profiles** 2.4.1 Configure user profiles 2.4.2 Configure Enterprise State Roaming in Azure AD **3.2 Manage Intune device enrollment and inventory** 3.2.6 Generate custom device inventory reports 3.2.7 Review device inventory	
10.4	Virtual Private Network (VPN)		
10.5	BitLocker		
10.6	Mobile Device Security	3.3 Monitor devices	

		3.3.1 Monitor device health (e.g., log analytics, Windows Analytics, or other cloud-based tools) 3.3.2 Monitor device security
10.7	Power Management	
10.8	Mobility Options	
10.9	Mobile Networking	
10.10	Mobile Apps	**4.1 Deploy and update applications** 4.1.1 Assign apps to groups 4.1.2 Deploy apps by using Intune 4.1.8 Configure and implement assigned access or public devices
10.11	Mobile Application Management with Intune	**4.2 Implement Mobile Application Management (MAM)** 4.2.1 Implement MAM policies 4.2.2 Manage MAM policies 4.2.3 Plan MAM 4.2.4 Configure Windows Information Protection 4.2.5 Implement Azure Information Protection templates 4.2.6 Securing data by using Intune
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 device health (e.g., log analytics, Windows Analytics, or other cloud-based tools) 3.3.2 Monitor device security
12.0	**System Protection**	
12.1	Windows Updates	**1.4 Manage updates** 1.4.3 Deploy Windows updates 1.4.4 Implement feature updates 1.4.5 Monitor Windows 10 updates
12.2	Advanced Windows Updates	**1.4 Manage updates** 1.4.1 Configure Windows 10 delivery optimization 1.4.2 Configure Windows Update for Business 1.4.3 Deploy Windows updates 1.4.5 Monitor Windows 10 updates
12.3	System Restore	
12.4	Backup	
12.5	Recovery	

12.6	Recovery Environment	
13.0	**Windows Defender**	
13.1	Malware Protection	3.1 Manage Windows Defender 3.1.6 Manage Windows Defender Antivirus
13.2	Windows Security	3.1 Manage Windows Defender 3.1.6 Manage Windows Defender Antivirus
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 Implement Windows Defender Advanced Threat Protection
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	

#	Domain	Module.Section
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	**Deploy and update operating systems**	
1.1	Plan and implement Windows 10 by using dynamic deployment 1.1.1 Evaluate and select an appropriate deployment option 1.1.2 Pilot deployment 1.1.3 Manage and troubleshoot provisioning packages	2.8 3.1, 3.3
1.2	Plan and implement Windows 10 by using Windows Autopilot 1.2.1 Evaluate and select an appropriate deployment option 1.2.2 Pilot deployment 1.2.3 Create, validate, and assign deployment profile 1.2.4 Extract device HW information to CSV file 1.2.5 Import device HW information to cloud service 1.2.6 Troubleshoot deployment	2.8
1.3	Upgrade devices to Windows 10 1.3.1 Identify upgrade and downgrade paths 1.3.2 Manage in-place upgrades 1.3.3 Configure a Windows analytics environment 1.3.4 Perform Upgrade Readiness assessment	2.6, 2.7

		1.3.5 Migrate user profiles	
1.4	Manage updates		12.1, 12.2
		1.4.1 Configure Windows 10 delivery optimization 1.4.2 Configure Windows Update for Business 1.4.3 Deploy Windows updates 1.4.4 Implement feature updates 1.4.5 Monitor Windows 10 updates	
1.5	Manage device authentication		4.1 8.5 10.3
		1.5.1 Manage authentication policies 1.5.2 Manage sign-on options 1.5.3 Perform Azure AD join	
2.0	**Manage policies and profiles**		
2.1	Plan and implement co-management		10.1
		2.1.1 Implement co-management precedence 2.1.2 Migrate group policy to MDM policies 2.1.3 recommend a co-management strategy	
2.2	Implement conditional access and compliance policies for devices		10.2, 10.3
		2.2.1 Implement conditional access policies 2.2.2 Manage conditional access policies 2.2.3 plan conditional access policies 2.2.4 Implement device compliance policies 2.2.5 Manage device compliance policies 2.2.6 plan device compliance policies	
2.3	Configure device profiles		10.3
		2.3.1 Implement device profiles	

		2.3.2 Manage device profiles 2.3.3 plan device profiles	
2.4	Manage user profiles 2.4.1 Configure user profiles 2.4.2 Configure Enterprise State Roaming in Azure AD 2.4.3 Configure sync settings 2.4.4 Implement Folder Redirection (including OneDrive)		5.4 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 Implement Windows Defender Advanced Threat Protection 3.1.5 Integrate Windows Defender Application Control 3.1.6 Manage Windows Defender Antivirus		8.4 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7
3.2	Manage Intune device enrollment and inventory 3.2.1 Configure enrollment settings 3.2.2 Configure Intune automatic enrollment 3.2.3 Enable device enrollment 3.2.4 Enroll non-Windows devices 3.2.5 Enroll Windows devices 3.2.6 Generate custom device inventory reports 3.2.7 Review device inventory		10.2, 10.3
3.3	Monitor devices 3.3.1 Monitor device health (e.g., log analytics, Windows Analytics, or other cloud-based tools) 3.3.2 Monitor device security		10.6 11.9

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 Intune 4.1.3 Deploy apps by using Microsoft Store for Business 4.1.4 Deploy O365 ProPlus 4.1.5 Enable sideloading of apps into images 4.1.6 Gather Office readiness data 4.1.7 Configure IE Enterprise mode 4.1.8 Configure and implement assigned access or public devices	2.5 3.4 7.3, 7.4 10.10
4.2	Implement Mobile Application Management (MAM) 4.2.1 Implement MAM policies 4.2.2 Manage MAM policies 4.2.3 Plan MAM 4.2.4 Configure Windows Information Protection 4.2.5 Implement Azure Information Protection templates 4.2.6 Securing data by using Intune	10.11