



# Device Security

Aa Area	⌚ Application	≡ Configurations	# Property	✓ Tested
<u>Essentials</u>	Accounts & Access	Local Administrator account is renamed or disabled	1.1	<input type="checkbox"/>
<u>Essentials</u>	Accounts & Access	Guest account is disabled	1.2	<input type="checkbox"/>
<u>Essentials</u>	Accounts & Access	User Account Control (UAC) is enabled	1.3	<input type="checkbox"/>
<u>Essentials</u>	Authentication	Require password complexity and minimum length	1.4	<input type="checkbox"/>
<u>Essentials</u>	Authentication	Limit password reuse and set maximum password age	1.5	<input type="checkbox"/>
<u>Essentials</u>	Authentication	Disable automatic login	1.6	<input type="checkbox"/>
<u>Essentials</u>	Lock Screen	Require password on wake-up from sleep	1.7	<input type="checkbox"/>
<u>Essentials</u>	BitLocker	BitLocker is enabled on system and data drives	1.8	<input type="checkbox"/>

Aa Area	⌚ Application	≡ Configurations	# Property	✓ Tested
<u>Essentials</u>	Updates	Windows Update is enabled and automatic	1.9	<input type="checkbox"/>
<u>Essentials</u>	Network	SMBv1 is disabled	1.1	<input type="checkbox"/>
<u>Essentials</u>	Remote Access	RDP is disabled unless specifically required	1.11	<input type="checkbox"/>
<u>Essentials</u>	Defender AV	Microsoft Defender Antivirus is enabled	1.12	<input type="checkbox"/>
<u>Essentials</u>	Defender AV	Cloud-delivered protection and automatic sample submission are enabled	1.13	<input type="checkbox"/>
<u>Essentials</u>	Smart Screen	Windows Defender SmartScreen is enabled	1.14	<input type="checkbox"/>
<u>Essentials</u>	Application Control	Only signed apps from trusted sources allowed	1.15	<input type="checkbox"/>
<u>Core</u>	Firewall	Windows Firewall is enabled and configured for all profiles	2.1	<input type="checkbox"/>
<u>Core</u>	Defender AV	Tamper protection is Enabled	2.2	<input type="checkbox"/>
<u>Core</u>	Attack Surface	Attack surface reduction rules applied via GPO or Intune	2.3	<input type="checkbox"/>
<u>Core</u>	Drive Encryption	BitLocker recovery information is stored securely (e.g., in Entra or AD)	2.4	<input type="checkbox"/>
<u>Core</u>	Updates	Devices are configured to use Windows Update for Business	2.5	<input type="checkbox"/>
<u>Core</u>	Applications	Windows Store access is restricted/managed	2.6	<input type="checkbox"/>
<u>Core</u>	Audit Policy	Audit object access, privilege use, logon events, and system events are enabled	2.7	<input type="checkbox"/>
<u>Core</u>	Lock Screen	Lock screen timeout is enforced after inactivity	2.8	<input type="checkbox"/>

Area	Application	Configurations	# Property	Tested
<u>Core</u>	Logging & Alerts	Windows Event Logging is enabled and monitored centrally	2.9	<input type="checkbox"/>
<u>Premium</u>	Hardening	Controlled Folder Access is enabled	3.1	<input type="checkbox"/>
<u>Premium</u>	Application Control	Application Control Policies (AppLocker or WDAC) are implemented	3.2	<input type="checkbox"/>
<u>Premium</u>	Credential Guard	Credential Guard is enabled on supported hardware	3.3	<input type="checkbox"/>
<u>Premium</u>	Device Control	USB and removable media restrictions in place via GPO or Intune	3.4	<input type="checkbox"/>
<u>Premium</u>	Defender AV	Defender AV periodic scanning is enforced, even with third-party AV installed	3.5	<input type="checkbox"/>
<u>Premium</u>	Privileged Access	LAPS (Local Admin Password Solution) is deployed and enforced	3.6	<input type="checkbox"/>
<u>Premium</u>	Updates	Feature updates are deferred per organization's update rings	3.7	<input type="checkbox"/>
<u>Premium</u>	Secure Boot	Secure Boot is enabled and enforced	3.8	<input type="checkbox"/>
<u>Advanced</u>	Threat Protection	Microsoft Defender for Endpoint is integrated and active	4.1	<input type="checkbox"/>
<u>Advanced</u>	Application Control	Full WDAC enforcement using managed policies	4.2	<input type="checkbox"/>
<u>Advanced</u>	Device Health	Integration with Microsoft Intune for compliance and health monitoring	4.3	<input type="checkbox"/>
<u>Advanced</u>	Isolation	Network isolation for untrusted apps and users (e.g., via App Container)	4.4	<input type="checkbox"/>

Aa Area	⌚ Application	≡ Configurations	# Property	✓ Tested
<u>Advan ced</u>	Credential Protection	Remote Credential Guard is enforced	4.5	<input type="checkbox"/>
<u>Advan ced</u>	Insider Risk	Insider risk policies are configured using Microsoft Purview	4.6	<input type="checkbox"/>
<u>Advan ced</u>	Logging & Analytics	Integration with SIEM/Sentinel for central log collection	4.7	<input type="checkbox"/>
<u>Advan ced</u>	Virtualization	Core Isolation and Memory Integrity are enabled	4.8	<input type="checkbox"/>
<u>Full Script</u>	Script			<input type="checkbox"/>
<u>Untitled</u>				<input type="checkbox"/>