Intune Documentation

SAMPLE REPORT, FICTIONAL TENANT

Technical Evidence Report: Intune Configuration

NCA ECC

ECC-2:2024

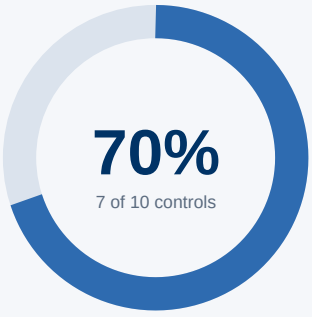
Evidence matrix for selected assessment points, read from the Microsoft Intune configuration

TENANT

Contoso Ltd

Report date **2026-10-08**

Classification **Internal**



Controls with supporting technical evidence

Supporting evidence only, not a compliance score

AT A GLANCE

Supporting or partial evidence	7
No recognized evidence	1
Mixed policy evidence	2

Evidence is read from the Microsoft Intune configuration export on the report date and mapped using ruleset 2026.11.19. Organizational aspects of each control are listed separately for review.

DOCUMENT CONTROL

Framework **NCA ECC ECC-2:2024**		Tenant **Contoso Ltd**	Prepared for **Information Security**
Prepared by **Endpoint Engineering**	Report ID **IDOC-ECC-20261008-CTSO**	Revision **1.0**	Ruleset version **2026.11.19**
Classification **Internal**	Report date **2026-10-08**		

01 EXECUTIVE SUMMARY

Summary

70%

CONTROLS WITH TECHNICAL EVIDENCE

7 of 10 assessable controls have supporting technical evidence in the Intune configuration.

41 of 64 technical safeguards are set up and switched on in Intune and Entra.

0 of 10 selected controls with configuration evidence (7 partial)
10 in scope; 0 outside the selected scope; 0 not assessed; 2 mixed policy evidence. Entries are selected mappings, not full framework coverage.
190 measures are outside Intune scope; each needs its own assessment.

0% 50% 100%

WITH TECHNICAL EVIDENCE	SAFEGUARDS IN PLACE	NO RECOGNIZED EVIDENCE	MIXED POLICY EVIDENCE
7	41	1	2
0 configuration, 7 supporting or partial	of 64 mapped, set up and switched on	controls without recognized evidence	controls with mixed policy evidence

Status distribution

10 controls



7 Supporting or partial evidence, 70% **1** No recognized evidence, 10% **2** Mixed policy evidence, 20%

Coverage by family

controls with technical evidence

ECC 2-2	Identity and access management		**2** of 2

5 more families are listed in the results overview.

Assigned deviating configurations: 3.
At least one assigned policy explicitly contradicts the target configuration.

Configured settings without assignment: 3.
The detected target configuration is not effective until it is assigned.

Key findings

ordered by severity, then control

- Assigned deviation · ECC 2-3-3-1 — **Office macro runtime scanning for all documents: Assigned deviating configuration affects ECC 2-3-3-1.**
- Assigned deviation · ECC 2-3-3-3 +1 — **Quality update timing within 14 days: Assigned deviating configuration affects ECC 2-3-3-3, ECC 2-10-3-4.**
- Assigned deviation · ECC 2-2-3-2 — **SMS, voice call and email one-time passcode not enabled for users (Entra ID): Assigned deviating configuration affects ECC 2-2-3-2.**
- Not assigned · ECC 2-3-2 — **Host firewall (Windows Firewall): Configured setting without assignment affects ECC 2-3-2.**
- Not assigned · ECC 2-3-2 — **System Integrity Protection: Configured setting without assignment affects ECC 2-3-2.**

1 further finding is listed in the full report.

SCOPE NOTE

This report documents technical evidence from the tenant's Microsoft Intune configuration. It is not a compliance certification and does not replace an audit. Missing evidence means that no supported configuration with a known assignment was detected in the evaluated dataset.

10 of 200 published requirements have Intune evidence mappings. Supporting evidence only; this is not a full assessment or compliance score.

02 RESULTS

Results Overview

Each selected control, its rolled up status, how many of its capabilities are evidenced, and where the supporting evidence is recorded.

CONTROL	STATUS	CAPABILITIES	EVIDENCE	PAGE
ECC 2-2 Identity and access management				2 of 2 with evidence
ECC 2-2-3-2 Multi-factor sign-in for remote and privileged access	Supporting or partial evidence	3 of 5	4 evidence items	n/a
ECC 2-2-3-4 Managing privileged access	Supporting or partial evidence	1 of 1	1 evidence item	n/a
ECC 2-3 Protection of systems and processing facilities				2 of 3 with evidence
ECC 2-3-2 Protection of workstations and systems in place	Supporting or partial evidence	10 of 20	15 evidence items	n/a
ECC 2-3-3-1 Antimalware and untrusted software control on endpoints	Supporting or partial evidence	12 of 16	17 evidence items	n/a
ECC 2-3-3-3 Keeping systems, apps and devices patched	Mixed policy evidence	1 of 2	4 evidence items	n/a
ECC 2-6 Mobile device security				2 of 2 with evidence
ECC 2-6-3-1 Separating and encrypting entity data on mobile devices	Supporting or partial evidence	4 of 5	7 evidence items	n/a
ECC 2-6-3-2 Restricting how mobile devices are used	Supporting or partial evidence	11 of 13	12 evidence items	n/a
ECC 2-8 Cryptography				1 of 1 with evidence
ECC 2-8-3-3 Encrypting stored data	Supporting or partial evidence	3 of 3	E-001 E-002 +4	4
ECC 2-10 Vulnerability management				0 of 1 with evidence
ECC 2-10-3-4 Installing updates that fix vulnerabilities	Mixed policy evidence	1 of 2	4 evidence items	n/a
ECC 2-12 Event logs and monitoring				0 of 1 with evidence
ECC 2-12-3-1 Security event logging on critical assets	No recognized evidence	0 of 4	None recorded	5

7 Supporting or partial evidence **1** No recognized evidence **2** Mixed policy evidence

Sample report: detail pages are included for selected controls only (ECC 2-8-3-3, ECC 2-12-3-1). A full report includes a detail page for every control. 190 measures are outside Intune scope; each needs its own assessment.

03 CONTROL DETAIL

ECC 2-8-3-3

Supporting or partial evidence

Encrypting stored data

6 match, 0 missing, 0 different

3 of 3 capabilities

6 evidence references

Disk encryption (BitLocker) Windows

Setting configured and assigned

CHECK	EXPECTED	ACTUAL	RESULT
Require Device Encryption device_vendor_msft_bitlocker_requiredeviceencryption WIN - Baseline - BitLocker	Enabled "device_vendor_msft_bitlocker_requiredeviceencryption_1"	**Enabled** "device_vendor_msft_bitlocker_requiredeviceencryption_1"	Matches expected value
BitLocker Enabled bitLockerEnabled WIN - Compliance - Baseline	true	**true**	Matches expected value

POLICY **WIN - Baseline - BitLocker** Assigned: Group: All Corporate Devices, Excluded: Group: Kiosk Devices

POLICY **WIN - Compliance - Baseline** Assigned: Group: All Corporate Devices

EVIDENCE E-001 E-002

Compliance requirement, not an observed device state. Marks noncompliant after 24 hours. Resource access depends on applicable Conditional Access policies; effective access is unverified.

Disk encryption (FileVault) macOS

Setting configured and assigned

CHECK	EXPECTED	ACTUAL	RESULT
Enable com.apple.mcx.filevault2_enable MAC - FileVault enforcement	On "com.apple.mcx.filevault2_enable_0"	**On** "com.apple.mcx.filevault2_enable_0"	Matches expected value
Force Enable In Setup Assistant com.apple.mcx.filevault2_forceenableinsetupassistant MAC - FileVault enforcement	True "com.apple.mcx.filevault2_forceenableinsetupassistant_true"	**True** "com.apple.mcx.filevault2_forceenableinsetupassistant_true"	Matches expected value
Storage Require Encryption storageRequireEncryption MAC - Compliance - Baseline	true	**true**	Matches expected value

POLICY **MAC - FileVault enforcement** Assigned: Group: Corporate Mac Devices

POLICY **MAC - Compliance - Baseline** Assigned: Group: Corporate Mac Devices

EVIDENCE E-003 E-004 E-005

Compliance requirement, not an observed device state. Marks noncompliant after 24 hours. Resource access depends on applicable Conditional Access policies; effective access is unverified.

Storage encryption (Android) Android

Compliance requirement assigned

CHECK	EXPECTED	ACTUAL	RESULT
Storage Require Encryption storageRequireEncryption AND - Compliance - Work profile	true	**true**	Matches expected value

POLICY **AND - Compliance - Work profile** Assigned: Group: Corporate Mobile Devices

EVIDENCE E-006

ECC 2-8-3-3 (continued)

Compliance requirement, not an observed device state. Marks noncompliant after 24 hours. Resource access depends on applicable Conditional Access policies; effective access is unverified.

Additional verification: not assessed by technical evidence

Encryption in transit, alignment with data classification and the National Cryptographic Standards, and key management need separate evidence.

ECC 2-12-3-1

No recognized evidence

Security event logging on critical assets

0 match, 4 missing, 0 different

0 of 4 capabilities

0 evidence references

Process creation auditing with command lines Windows

No evidence

CHECK	EXPECTED	ACTUAL	RESULT
Process creation auditing with command lines windows-process-creation-logging	"Success" or "Success+ Failure"; alternative: "Enabled"	*Not found*	Missing

No supported setting was found after checking the collected policies.

POLICY No matching policy found

EVIDENCE None recorded

PowerShell logging for all modules Windows

No evidence

CHECK	EXPECTED	ACTUAL	RESULT
PowerShell logging for all modules windows-powershell-module-logging	"*"; requires Turn on Module Logging: Enabled	*Not found*	Missing

No supported setting was found after checking the collected policies.

POLICY No matching policy found

EVIDENCE None recorded

PowerShell script block logging enabled Windows

No evidence

CHECK	EXPECTED	ACTUAL	RESULT
PowerShell script block logging enabled windows-powershell-scriptblock-logging	"Enabled"	*Not found*	Missing

No supported setting was found after checking the collected policies.

POLICY No matching policy found

EVIDENCE None recorded

ECC 2-12-3-1 (continued)

PowerShell transcription enabled Windows

No evidence

CHECK	EXPECTED	ACTUAL	RESULT
PowerShell transcription enabled windows-powershell-transcription	"Enabled"	*Not found*	Missing

No supported setting was found after checking the collected policies.

POLICY	No matching policy found
EVIDENCE	None recorded

Gap: Security event logging on critical assets

No technical evidence was found. Possible implementation through these Intune settings:

- device_vendor_msft_policy_config_audit_detailedtracking_auditprocesscreation
- device_vendor_msft_policy_config_admx_auditsettings_includecmdline
- device_vendor_msft_policy_config_admx_powershellexecutionpolicy_enablemodulelogging_listbox_modulenames
- device_vendor_msft_policy_config_windowspowershell_turnonpowershellscriptblocklogging

Additional verification: not assessed by technical evidence

Which assets are critical, central collection in a SIEM, continuous monitoring and keeping logs for at least 12 months need separate evidence.

HOW TO READ THIS REPORT

Configuration evidence	Technical configuration evidence detected
Supporting or partial evidence	Technical configuration evidence partially detected
No recognized evidence	No supported technical configuration evidence detected
Mixed policy evidence	Mixed policy evidence
Not assessed	Not assessed
Outside selected scope	Outside selected scope

1. Status is shown by marker shape and label, never by colour alone.
2. A control rolls up from its capabilities. A capability rolls up from its checks.
3. Only assigned policies count as evidence. Configured but unassigned settings are reported separately.
4. Evidence references point to rows of the evidence register in Appendix A.

APPENDIX A

Appendix A: Evidence Register

Every configuration value cited in this report, as read from the tenant export. References are stable within a report ID.

REF	POLICY	TYPE	SETTING	VALUE	ASSIGNMENT
E-001	WIN - Baseline - BitLocker 0c0e7050-0000-4000-8000-000000000101; configuration; version unknown; modified 2026-08-19T14:30:00Z	Settings Catalog	Require Device Encryption device_vendor_msft_bitlocker_requireddeviceencryption	**Enabled** device_vendor_msft_bitlocker_requiredeviceencryption_1	Group: All Corporate Devices, Excluded: Group: Kiosk Devices
E-002	WIN - Compliance - Baseline 0c0e7050-0000-4000-8000-000000000301; complianceRequirement; version 4; modified 2026-08-12T10:00:00Z	Compliance Policy	BitLocker Enabled bitLockerEnabled	**true**	Group: All Corporate Devices
E-003	MAC - FileVault enforcement 0c0e7050-0000-4000-8000-000000000109; configuration; version unknown; modified 2026-06-18T10:45:00Z	Settings Catalog	Enable com.apple.mcx.filevault2_enable	**On** com.apple.mcx.filevault2_enable_0	Group: Corporate Mac Devices
E-004	MAC - FileVault enforcement 0c0e7050-0000-4000-8000-000000000109; configuration; version unknown; modified 2026-06-18T10:45:00Z	Settings Catalog	Force Enable In Setup Assistant com.apple.mcx.filevault2_forceenableinsetupassistant	**True** com.apple.mcx.filevault2_forceenableinsetupassistant_true	Group: Corporate Mac Devices
E-005	MAC - Compliance - Baseline 0c0e7050-0000-4000-8000-000000000302; complianceRequirement; version 3; modified 2026-06-18T11:00:00Z	Compliance Policy	Storage Require Encryption storageRequireEncryption	**true**	Group: Corporate Mac Devices
E-006	AND - Compliance - Work profile 0c0e7050-0000-4000-8000-000000000305; complianceRequirement; version 3; modified 2026-07-30T09:45:00Z	Compliance Policy	Storage Require Encryption storageRequireEncryption	**true**	Group: Corporate Mobile Devices

Referenced assessment points for each item of evidence are listed in the relevant sections.

ANNEX

Policy device status

Device counts as summarised by Intune for the device policies cited in this report. Context only: no status in this report depends on them, and they do not show the state of an individual device. Errors include devices reported as not compliant. No status reported means the Intune summary has no row for the policy, not a count of zero.

Status summaries read on 2026-10-08T09:00:00Z. Configuration report: collected. Compliance report: collected. Profile status overview: collected.

POLICY	SOURCE	SUCCEEDED	ERRORS	CONFLICTS	NOT APPLICABLE	PENDING
WIN - Baseline - BitLocker	Configuration report	**412**	**6**	**2**	**3**	**n/a**
WIN - Compliance - Baseline	Compliance report	**401**	**22**	**0**	**0**	**n/a**
MAC - FileVault enforcement	Configuration report	**58**	**3**	**0**	**0**	**n/a**
MAC - Compliance - Baseline	Compliance report	**57**	**4**	**0**	**0**	**n/a**
AND - Compliance - Work profile	Compliance report	**87**	**5**	**0**	**0**	**n/a**

APPENDIX B

Methodology

Evidence is determined exclusively from concrete Intune settings: An assessment point is considered technically evidenced only when a recognized setting is configured with a recognized value and the policy is assigned. Configurations that explicitly contradict the target state are reported separately. Unsupported settings or settings that cannot be mapped unambiguously remain unassessed. Organizational requirements are not part of this automated technical assessment and must be assessed separately.

Note: Supporting device-management and Entra ID evidence for selected Cybersecurity Defense controls of the Essential Cybersecurity Controls (108 main controls and 92 subcontrols). Governance, resilience, third-party and cloud controls and the many process controls are organisational and outside the scope of an Intune tenant export. Source: National Cybersecurity Authority (NCA), Essential Cybersecurity Controls ECC-2:2024. Titles and summaries paraphrased; only the Arabic text is binding.