Intune Documentation

SAMPLE REPORT, FICTIONAL TENANT

Technical Evidence Report: Intune Configuration

DORA

Regulation (EU) 2022/2554 and RTS (EU) 2024/1774

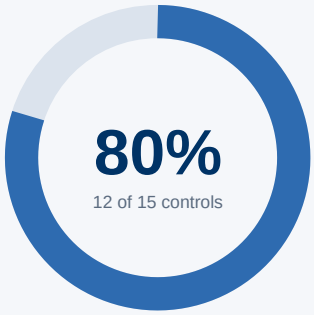
Evidence matrix for selected assessment points, read from the Microsoft Intune configuration

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	12
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 2026.10.22. Organizational aspects of each control are listed separately for review.

DOCUMENT CONTROL

Framework	**Tenant**	**Prepared for**	
DORA Regulation (EU) 2022/2554 and RTS (EU) 2024/1774	Contoso Ltd	Information Security	
Prepared by	**Report ID**	**Revision**	**Ruleset version**
Endpoint Engineering	IDOC-DORA-20261008-CTSO	1.0	2026.10.22
Classification	**Report date**		
Internal	2026-10-08		

01 EXECUTIVE SUMMARY

Summary

80%

CONTROLS WITH TECHNICAL EVIDENCE

12 of 15 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 15 selected controls with configuration evidence (12 partial)
15 in scope; 0 outside the selected scope; 0 not assessed; 2 mixed policy evidence. Entries are selected mappings, not full framework coverage.
8 measures are outside Intune scope; each needs its own assessment.



WITH TECHNICAL EVIDENCE	SAFEGUARDS IN PLACE	NO RECOGNIZED EVIDENCE	MIXED POLICY EVIDENCE
12	41	1	2
0 configuration, 12 supporting or partial	of 64 mapped, set up and switched on	controls without recognized evidence	controls with mixed policy evidence

Status distribution

15 controls



12 Supporting or partial evidence, 80% **1** No recognized evidence, 7% **2** Mixed policy evidence, 13%

Coverage by family

controls with technical evidence

DORA Art. 9	Regulation (EU) 2022/2554	**3** of 4
DORA Art. 10	Regulation (EU) 2022/2554	**0** of 1

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 · RTS 11(2)(d) — **Office macro runtime scanning for all documents: Assigned deviating configuration affects RTS 11(2)(d).**
- Assigned deviation · DORA 9(4)(f) · +1 — **Quality update timing within 14 days: Assigned deviating configuration affects DORA 9(4)(f), RTS 10(4)(c).**
- Assigned deviation · DORA 9(4)(d) · +1 — **SMS, voice call and email one-time passcode not enabled for users (Entra ID): Assigned deviating configuration affects DORA 9(4)(d), RTS 21(f)(ii).**
- Not assigned · RTS 11(2)(b) — **Host firewall (Windows Firewall): Configured setting without assignment affects RTS 11(2)(b).**
- Not assigned · RTS 11(2)(b) — **System Integrity Protection: Configured setting without assignment affects RTS 11(2)(b).**

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.

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
DORA Art. 9 Regulation (EU) 2022/2554				3 of 4 with evidence
DORA 9(2) Protecting data at rest, in use and in transit	Supporting or partial evidence	3 of 3	6 evidence items	n/a
DORA 9(4)(c) Limiting logical access to what is needed	Supporting or partial evidence	9 of 11	9 evidence items	n/a
DORA 9(4)(d) Strong authentication policies	Supporting or partial evidence	3 of 5	4 evidence items	n/a
DORA 9(4)(f) Patch and update policies	Mixed policy evidence	1 of 2	4 evidence items	n/a
DORA Art. 10 Regulation (EU) 2022/2554				0 of 1 with evidence
DORA 10(1) Detecting anomalous activities	No recognized evidence	0 of 4	None recorded	4
RTS Art. 6 Delegated Regulation (EU) 2024/1774				1 of 1 with evidence
RTS 6(2)(a) Encryption of data at rest and in transit	Supporting or partial evidence	3 of 3	6 evidence items	n/a
RTS Art. 10 Delegated Regulation (EU) 2024/1774				0 of 1 with evidence
RTS 10(4)(c) Testing and deploying patches	Mixed policy evidence	1 of 2	4 evidence items	n/a
RTS Art. 11 Delegated Regulation (EU) 2024/1774				4 of 4 with evidence
RTS 11(2)(b) Secure configuration baseline	Supporting or partial evidence	12 of 22	18 evidence items	n/a
RTS 11(2)(c) Only authorised software installed	Supporting or partial evidence	1 of 4	2 evidence items	n/a
RTS 11(2)(d) Protection against malicious code	Supporting or partial evidence	11 of 12	15 evidence items	n/a
RTS 11(2)(e) Authorised storage and transfer of data	Supporting or partial evidence	1 of 2	1 evidence item	n/a
RTS Art. 13 Delegated Regulation (EU) 2024/1774				2 of 2 with evidence
RTS 13(d) Blocking non-compliant endpoints	Supporting or partial evidence	1 of 1	1 evidence item	n/a
RTS 13(l) Session lock after inactivity	Supporting or partial evidence	3 of 4	E-001 E-002 E-003	5
RTS Art. 21 Delegated Regulation (EU) 2024/1774				2 of 2 with evidence
RTS 21(e)(ii) Privileged access on a need-to-use basis	Supporting or partial evidence	1 of 1	1 evidence item	n/a
RTS 21(f)(ii) Strong authentication for remote and privileged access	Supporting or partial evidence	3 of 5	4 evidence items	n/a

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

Sample report: detail pages are included for selected controls only (DORA 10(1), RTS 13(l)). A full report includes a detail page for every control.
8 measures are outside Intune scope; each needs its own assessment.

03 CONTROL DETAIL

DORA 10(1)

No recognized evidence

Detecting anomalous activities

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

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

DORA 10(1) (continued)

Gap: Detecting anomalous activities

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

Central collection, alerting, response, detection of single points of failure and regular testing of the detection mechanisms need separate evidence.

RTS 13(l)

Supporting or partial evidence

Session lock after inactivity

3 match, 1 missing, 0 different

3 of 4 capabilities

3 evidence references

Screen lock after inactivity (Windows) Windows

No evidence

CHECK	EXPECTED	ACTUAL	RESULT
Screen lock after inactivity (Windows) windows-inactivity-lock	At least 1; requires Device Password Enabled: Enabled; alternative: At least 1	*Not found*	Missing

No supported setting was found after checking the collected policies.

POLICY No matching policy found

EVIDENCE None recorded

Screen lock after inactivity (macOS) macOS

Compliance requirement assigned

A configured inactivity limit locks the screen; it does not sign the user out or end the session. Whether the limit meets the organisation's required period is not assessed.

CHECK	EXPECTED	ACTUAL	RESULT
Password Minutes Of Inactivity Before Lock passwordMinutesOfInactivityBeforeLock MAC - Compliance - Baseline	At least 1	**5**	Matches expected value

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

EVIDENCE E-001

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

RTS 13(l) (continued)

Screen lock after inactivity (iOS/iPadOS) iOS

Compliance requirement assigned

A configured inactivity limit locks the screen; it does not sign the user out or end the session. Whether the limit meets the organisation's required period is not assessed.

CHECK	EXPECTED	ACTUAL	RESULT
Passcode Minutes Of Inactivity Before Screen Timeout passcodeMinutesOfInactivityBeforeScreenTimeout iOS - Compliance - Baseline	At least 1	**2**	Matches expected value

POLICY **iOS - Compliance - Baseline** Assigned: Group: Corporate Mobile Devices

EVIDENCE 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.

Screen lock after inactivity (Android) Android

Compliance requirement assigned

A configured inactivity limit locks the screen; it does not sign the user out or end the session. Whether the limit meets the organisation's required period is not assessed.

CHECK	EXPECTED	ACTUAL	RESULT
Password Minutes Of Inactivity Before Lock passwordMinutesOfInactivityBeforeLock AND - Compliance - Work profile	At least 1	**5**	Matches expected value

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

EVIDENCE E-003

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

Ending system and remote sessions, the organisation's defined period and remote access session limits need separate evidence.

A configured inactivity limit locks the screen; it does not sign the user out or end the session. Whether the limit meets the organisation's required period is not assessed.

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	MAC - Compliance - Baseline 0c0e7050-0000-4000-8000-000000000302; complianceRequirement; version 3; modified 2026-06-18T11:00:00Z	Compliance Policy	Password Minutes Of Inactivity Before Lock passwordMinutesOfInactivityBeforeLock	**5**	Group: Corporate Mac Devices
E-002	iOS - Compliance - Baseline 0c0e7050-0000-4000-8000-000000000304; complianceRequirement; version 5; modified 2026-07-30T09:30:00Z	Compliance Policy	Passcode Minutes Of Inactivity Before Screen Timeout passcodeMinutesOfInactivityBeforeScreenTimeout	**2**	Group: Corporate Mobile Devices
E-003	AND - Compliance - Work profile 0c0e7050-0000-4000-8000-000000000305; complianceRequirement; version 3; modified 2026-07-30T09:45:00Z	Compliance Policy	Password Minutes Of Inactivity Before Lock passwordMinutesOfInactivityBeforeLock	**5**	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
MAC - Compliance - Baseline	Compliance report	**57**	**4**	**0**	**0**	**n/a**
iOS - Compliance - Baseline	Compliance report	**233**	**9**	**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 ICT risk management points of DORA Art. 9 and 10 and of the RTS on the ICT risk management framework. Governance, risk management framework, incident reporting, resilience testing, third-party risk and information sharing are organisational and outside the scope of an Intune tenant export. Source: EUR-Lex, Regulation (EU) 2022/2554 and Commission Delegated Regulation (EU) 2024/1774. Titles paraphrased; only the Official Journal text is authentic.