utilITise IT Health Assessment Report

Read-Only

EVALUATED BY D.O.N.N.A.



GOOD

Identity	29/30
Devices	23/25
Security	24/30
Operations	12/15

16 AUTOMATED CHECKS

- 12 Pass
- 3 Attention
- 1 At risk

KEY METRICS

7
USERS WITHOUT MFA
of 25 active users

1
DEVICES NOT SYNCED 60+ DAYS
of 20 managed devices

1
STALE ACCOUNTS, INACTIVE
of 25 enabled users

3
NON-COMPLIANT DEVICES
of 20 devices

TOP ISSUES

HIGH	Users without MFA set up	28%
HIGH	Repeated sign-in failures	4%
MEDIUM	Stale enabled accounts	4%
MEDIUM	Non-compliant devices enrolled	15%
MEDIUM	Devices running outdated OS versions	10%

SELF-HEALING REMEDIATION PLAN

+ Users without MFA set up
+ Repeated sign-in failures
+ Stale enabled accounts
+ Non-compliant devices enrolled
+ Devices running outdated OS versions

With Self-Healing IT enabled

Projected outcome once D.O.N.N.A. completes the plan above.

99

10.0+
hrs saved

$450
value saved

Scoring Matrix

Pass · Attention · At risk

16 automated checks across 4 categories. Each check is evaluated by D.O.N.N.A. from live tenant data.

Identity — 29 / 30

Admin accounts (2 configured)	5 / 5
MFA enrollment — 72.0% of users registered	4 / 5
Stale accounts — 1 inactive 90+ days	5 / 5
Account-recovery registration — 92.0% of users registered	5 / 5
Recovery contacts — 0 privileged account(s) missing	5 / 5

Devices — 23 / 25

Compliance — 85.0% of 20 devices	3 / 4
Disk encryption coverage — 95.0%	4 / 4
Sync freshness — 5.0% not synced 60+ days	4 / 4
OS currency — 90.0% up to date	4 / 4

Security — 24 / 30

Conditional Access — 4/4 baselines met	5 / 5
Risk detections — 1 account(s) flagged	3 / 5
Inactive admin review — 0 inactive	5 / 5
Threat protection — 60.0% of Secure Score controls enabled	3 / 5

Operations — 12 / 15

Group hygiene — 0 ownerless group(s)	3 / 3
Mailbox health — 0 near storage quota	3 / 3
Inactive devices — 1 retirement candidate(s) (90+ days)	1 / 3

Total IT Health Score **88 / 100**

Detailed Findings Appendix

Executive Summary — Top 5 Risks

Rank	Severity	Risk	Description
#1	High	Users without MFA set up	7 of 25 user(s) (28.0%) have not set up an MFA method.
#2	High	Repeated sign-in failures	1 of 25 enabled user(s) (4.0%) had 3 or more failed sign-in attempts in the last 7 days.
#3	Medium	Stale enabled accounts	1 enabled account(s) (4.0%) have had no sign-in activity for over 90 days.
#4	Medium	Non-compliant devices enrolled	3 of 20 device(s) (15.0%) are non-compliant.
#5	Medium	Devices running outdated OS versions	2 of 20 device(s) (10.0%) are behind on OS patch levels.

Conditional Access Policies

4 enabled policies out of 4 total.

Baseline	Status
Require MFA for administrators	**Met**
Block legacy authentication	**Met**
Require MFA for all users	**Met**
Require compliant device for access	**Met**

MFA Coverage

18 of 25 user(s) (72.0%) have an MFA method registered; 7 have not set one up yet.

All privileged accounts have MFA registered.

Stale Accounts & Offboarding

1 of 25 enabled account(s) have had no sign-in activity for an extended period.

Device Compliance

85.0% of 20 device(s) are compliant, across 4 compliance policies.

Device	OS	User
KRP-LT-005	Windows	connor.walsh@kestrelridge.co
KRP-LT-011	Windows	brian.fischer@kestrelridge.co
KRP-IPH-003	iOS	sarah.collins@kestrelridge.co

Patch Status

10.0% of 20 device(s) are behind on OS patch levels.

Device	OS	Version
KRP-LT-005	Windows	10.0.19044.3086
KRP-LT-011	Windows	10.0.19044.2965