WINTIVE

M365 Tenant Health Check

Automated audit report for **Sample SMB / Manufacturing / 50 users**

Audit ID: cs_sample_showcase_001 · 2026-04-28 13:38 UTC · v1.0

by WINTIVE LLC Microsoft Verified Publisher
nicolas@wintive.com · https://www.wintive.com

Executive summary

22/100

At risk

5 passed · **22** to fix · **27** live checks of 50 declared

Findings by severity

SEVERITY	FAILURES	RECOMMENDED ACTION
CRITICAL	**7**	Address within 24 hours
HIGH	**9**	Address within 1 week
MEDIUM	**4**	Address within 1 month
LOW	**2**	Backlog / next review

Top 5 findings to fix this week

1. CRITICAL #01 **Security Defaults OR Conditional Access enabled**
2. CRITICAL #02 **Legacy authentication blocked**
3. CRITICAL #03 **Break-glass (emergency) account exists**
4. CRITICAL #06 **Risky sign-in & risky user policies enabled**
5. CRITICAL #08 **Guest access governance**

Licensing posture

Your tenant currently holds:

- **Microsoft 365 Business Premium** — 25 seats
- **Exchange Online Plan 1** — 5 seats

Of your 22 findings to fix:

21 ✅ fixable immediately with current licensing

1 🚫 require a licensing upgrade

Recommended upgrade path: adding **Microsoft 365 E5** would unlock 1 of the 1 licensing-blocked finding.

Contents

1. Entra ID & Identity

Checks #01–#10 · 10 total

#01 Security Defaults OR Conditional Access enabled

CRITICAL FAIL

Configuration gap detected on check #01: Security Defaults OR Conditional Access enabled. Remediation guidance below.

```
Entra admin center → Identity → Overview → Properties → Manage security defaults
→ enable. For E3/Business Premium, prefer a Conditional Access policy requiring
MFA for all users on all cloud apps.
```

✅ **Licensing:** Security Defaults free for any tenant; Conditional Access requires Entra ID P1 (included in Business Premium / E3+).

[See evidence]

#02 Legacy authentication blocked

CRITICAL FAIL

Configuration gap detected on check #02: Legacy authentication blocked. Remediation guidance below.

```
Entra admin center → Protection → Conditional Access → New policy. Users: All.
Cloud apps: All. Conditions → Client apps: tick 'Other clients'. Grant: Block.
Legacy protocols (SMTP AUTH, IMAP, POP3) bypass MFA entirely without this gate.
```

POWERSHELL ALTERNATIVE

```
# Audit existing CA policies that target legacy clients (Connect-MgGraph -Scopes
Policy.Read.All):
Get-MgIdentityConditionalAccessPolicy | Where { $_.Conditions.ClientAppTypes -contains
'other' } | Select DisplayName, State
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#03 Break-glass (emergency) account exists

CRITICAL FAIL

Configuration gap detected on check #03: Break-glass (emergency) account exists. Remediation guidance below.

```
Create 1-2 cloud-only Global Admin accounts (breakglass-1, breakglass-2) with 64+
char passwords stored in a physical safe. Exclude from all Conditional Access
policies. Without break-glass, an MFA outage locks you out of your own tenant.
```

✅ **Licensing:** No special license required.

[See evidence]

#04 MFA enforced for all administrators

CRITICAL PASS

Configuration valid — no action required.

#05 Self-service password reset enabled

CRITICAL ERROR

This check could not complete because the Microsoft Graph endpoint returned an unexpected response. This is often a tenant license tier limitation or a feature that has not been configured.

```
Contact s***@w***.com with this report's reference; we'll re-run the failing check at no charge.
```

#06 Risky sign-in & risky user policies enabled

CRITICAL FAIL

Configuration gap detected on check #06: Risky sign-in & risky user policies enabled. Remediation guidance below.

```
Entra admin center → Protection → Conditional Access → Templates: enable 'Require MFA for high sign-in risk' AND 'Require password change for high user risk'. Identity Protection signals (impossible travel, leaked credentials) trigger nothing without these policies.
```

🚫 **Licensing:** Requires Entra ID P2 (in Microsoft 365 E5 or Entra ID P2 add-on).

[See evidence]

#07 Privileged Identity Management configured

CRITICAL ERROR

This check could not complete because the Microsoft Graph endpoint returned an unexpected response. This is often a tenant license tier limitation or a feature that has not been configured.

```
Contact s***@w***.com with this report's reference; we'll re-run the failing check at no charge.
```

#08 Guest access governance

CRITICAL FAIL

Configuration gap detected on check #08: Guest access governance. Remediation guidance below.

```
Entra admin center → External Identities → External collaboration settings: set 'Guest user access' to 'limited access' and require admin approval for invites. Default settings let any user invite externals who can then read directory metadata.
```

✅ **Licensing:** No special license required.

[See evidence]

#09 Admin role count ≤ 5

CRITICAL FAIL

Configuration gap detected on check #09: Admin role count ≤ 5. Remediation guidance below.

```
Entra admin center → Roles & admins → Global administrator: audit assignments and remove any not actively needed. Aim for ≤5 standing Global Admins; more = wider blast radius on a single compromise.
```

POWERSHELL ALTERNATIVE

```
# Count Global Admin assignments (Connect-MgGraph -Scopes RoleManagement.Read.Directory):
$ga = Get-MgDirectoryRole -Filter "displayName eq 'Global Administrator'"
(Get-MgDirectoryRoleMember -DirectoryRoleId $ga.Id).Count
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#10 Conditional Access policy hygiene

CRITICAL FAIL

Configuration gap detected on check #10: Conditional Access policy hygiene. Remediation guidance below.

```
Entra admin center → Conditional Access → Policies: review every active policy for stale user exclusions, overlapping rules, and 'report-only' modes never promoted. Each unused exclusion is a permanent bypass; consolidate or retire policies quarterly.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

2. Exchange Online & Mail Flow

Checks #11–#18 · 8 total

#11 SPF DNS record published with hard fail

HIGH FAIL

Configuration gap detected on check #11: SPF DNS record published with hard fail. Remediation guidance below.

```
Add a TXT record at your domain root: v=spf1 include:spf.protection.outlook.com -all (note the -all hard fail, not ~all soft fail). Validate with dig +short TXT yourdomain.com or mxtoolbox.com SPF Check.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#12 DKIM enabled for all sending domains

HIGH FAIL

Configuration gap detected on check #12: DKIM enabled for all sending domains. Remediation guidance below.

Defender → Email & collaboration → Threat policies → DKIM: enable signing for each accepted domain, then publish the two selector1/selector2 CNAME records at your DNS. Validate: dig +short CNAME selector1._domainkey.yourdomain.com.

POWERSHELL ALTERNATIVE

```
# Connect-ExchangeOnline first. Run per verified sending domain:
Set-DkimSigningConfig -Identity yourdomain.com -Enabled $true
Get-DkimSigningConfig | Select Domain, Enabled, Selector1CNAME, Selector2CNAME
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#13 DMARC record published (p=quarantine or p=reject)

HIGH WARNING

Partial configuration detected on check #13: DMARC record published (p=quarantine or p=reject). Improvement guidance below.

Improvement: Add a TXT record at _dmarc.yourdomain.com: v=DMARC1; p=quarantine; rua=mailto:dmarc@yourdomain.com; pct=100. Start with quarantine, monitor rua reports 2-4 weeks, then tighten to p=reject. Validate: dig +short TXT _dmarc.yourdomain.com.

POWERSHELL ALTERNATIVE

```
# Validate DMARC TXT after publishing (no Connect-* required, native PS):
Resolve-DnsName -Type TXT -Name "_dmarc.yourdomain.com" | Select Strings
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

HIGH	V1.1	#14	Anti-phishing policy with impersonation protection
HIGH	V1.1	#15	Safe Attachments and Safe Links enabled
HIGH	V1.1	#16	Outbound spam policy limits configured
HIGH	V1.1	#17	Mailbox auditing enabled
HIGH	V1.1	#18	Auto-forwarding to external blocked

3. SharePoint & OneDrive

Checks #19–#25 · 7 total

#19 Default sharing capability not 'Anyone with the link'

MEDIUM FAIL

Configuration gap detected on check #19: Default sharing capability not 'Anyone with the link'. Remediation guidance below.

```
SharePoint admin center → Policies → Sharing. Under 'External sharing — SharePoint', move the slider to 'New and existing guests' (default safe) or stricter. Anyone-with-the-link surfaces tenant content to crawlers and ex-employees.
```

POWERSHELL ALTERNATIVE

```
# Tighten tenant-wide sharing in one line (Connect-SPOService -Url https://-admin.sharepoint.com first):
Set-SPOTenant -SharingCapability ExistingExternalUserSharingOnly
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#20 External sharing notifications routed to admin

MEDIUM FAIL

Configuration gap detected on check #20: External sharing notifications routed to admin. Remediation guidance below.

```
SharePoint admin center → Policies → Sharing: enable 'Notify owners when files / folders are shared'. Plus enable tenant-wide audit log. Without alerts, a phished user inviting an attacker as a guest goes unnoticed for weeks.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

MEDIUM V1.1 #21 Sharing capability set to Existing Guests Only

MEDIUM V1.1 #22 External user expiration policy configured

#23 Sensitivity labels published and applied

MEDIUM ERROR

This check could not complete because the Microsoft Graph endpoint returned an unexpected response. This is often a tenant license tier limitation or a feature that has not been configured.

```
Contact s***@w***.com with this report's reference; we'll re-run the failing check at no charge.
```

#24 Anonymous link expiration ≤ 30 days

MEDIUM FAIL

Configuration gap detected on check #24: Anonymous link expiration ≤ 30 days. Remediation guidance below.

```
SharePoint admin center → Policies → Sharing → Anyone-link defaults: expiration 30 days max, permissions View only. Permanent Anyone-links are a slow-motion data leak as documents drift via forwards.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#25 OneDrive retention policy enforced

MEDIUM PASS

Configuration valid — no action required.

4. Microsoft Teams

Checks #26–#31 · 6 total

MEDIUM V1.1 #26 Federation with external organizations limited

MEDIUM V1.1 #27 Anonymous meeting join policy

MEDIUM V1.1 #28 Teams app permission policy enforced

MEDIUM V1.1 #29 Teams external file sharing policy

#30 Teams meeting recording auto-policy

MEDIUM FAIL

Configuration gap detected on check #30: Teams meeting recording auto-policy. Remediation guidance below.

```
Teams admin center → Meetings → Meeting policies: under 'Recording & transcription', set 'Cloud recording' to On and 'Transcription' to On. Define retention via Purview retention policy (e.g. 90 days). Recordings are evidence in HR / IP disputes.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

MEDIUM V1.1 #31 Live events policy hardened

5. Intune & Device Management

Checks #32–#39 · 8 total

#32 Device compliance enforced via Conditional Access

HIGH FAIL

Configuration gap detected on check #32: Device compliance enforced via Conditional Access. Remediation guidance below.

```
Pair an Intune compliance policy (Endpoint Manager → Devices → Compliance policies) defining 'compliant' (encryption, OS version, threat level) with a Conditional Access policy: Users All / Cloud apps All / Grant: Require device to be marked as compliant.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#33 Disk encryption required (BitLocker / FileVault)

HIGH FAIL

Configuration gap detected on check #33: Disk encryption required (BitLocker / FileVault). Remediation guidance below.

```
Endpoint Manager → Devices → Compliance policies: create per-platform policy requiring BitLocker (Windows) / FileVault (macOS) + minimum OS version. Pair with #32 CA. Unencrypted stolen laptops = full data breach + GDPR notification.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#34 Compliance policy applied to all platforms

HIGH FAIL

Configuration gap detected on check #34: Compliance policy applied to all platforms. Remediation guidance below.

```
Endpoint Manager → Devices → Compliance policies: ensure one per supported
platform (Windows, macOS, iOS, Android). Without per-platform policy,
compliant=true is granted by default for that platform — Conditional Access #32
has no teeth there.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#35 Microsoft Defender for Endpoint deployed

HIGH FAIL

Configuration gap detected on check #35: Microsoft Defender for Endpoint deployed. Remediation guidance below.

```
Endpoint Manager → Endpoint security → Antivirus: create a 'Microsoft Defender
Antivirus' profile assigned to all devices. Plus 'Endpoint detection and
response' with cloud-attached protection on. Built-in Defender is base AV; EDR
adds the cloud signal layer.
```

✅ **Licensing:** Either MDE_SMB (in Microsoft 365 Business Premium) OR WINDEFATP (in M365 E5 / Defender for Endpoint P1+) satisfies; pick whichever your tenant has.

[See evidence]

#36 Windows Autopilot enrolment configured

HIGH ERROR

This check could not complete because the Microsoft Graph endpoint returned an unexpected response. This is often a tenant license tier limitation or a feature that has not been configured.

```
Contact s***@w***.com with this report's reference; we'll re-run the failing check at no charge.
```

#37 Intune device enrolment restrictions set

HIGH FAIL

Configuration gap detected on check #37: Intune device enrolment restrictions set. Remediation guidance below.

```
Endpoint Manager → Devices → Enrollment → Device platform restrictions: block personal-owned iOS/Android unless approved. Set per-user enrolment limit to 5. Without limits, an attacker with creds can flood Intune with rogue devices.
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

HIGH V1.1 #38 Lost/stolen device wipe procedure documented

#39 Mobile app management (MAM) policy applied

HIGH PASS

Configuration valid — no action required.

6. License Posture & Cost Control

Checks #40–#44 · 5 total

#40 Unassigned licenses ≤ 5% of total

LOW WARNING

Partial configuration detected on check #40: Unassigned licenses ≤ 5% of total. Improvement guidance below.

Improvement: M365 admin center → Billing → Licenses: review each SKU 'Unassigned' count. For >5% unassigned (excl. trial/free), reduce seat count at next renewal. Trial/free SKUs auto-provisioned by Microsoft don't count.

POWERSHELL ALTERNATIVE

```
# Bulk audit consumed-vs-prepaid per SKU (Connect-MgGraph -Scopes Organization.Read.All):
Get-MgSubscribedSku | Select SkuPartNumber, @{n='Consumed';e={$_.ConsumedUnits}},
@{n='Total';e={$_.PrepaidUnits.Enabled}}, @{n='Unused';e={$_.PrepaidUnits.Enabled -
$_.ConsumedUnits}}
```

✅ **Licensing:** No special license required.

[See evidence]

#41 Inactive accounts retain assigned licenses

LOW FAIL

Configuration gap detected on check #41: Inactive accounts retain assigned licenses. Remediation guidance below.

M365 admin center → Active users → filter inactive (last sign-in > 90 days). Remove license from each (keeps user, frees seat). Compounds cost saving; idle licensed accounts are also unmonitored attack vectors.

POWERSHELL ALTERNATIVE

```
# List licensed users with no sign-in for 90+ days (Connect-MgGraph -Scopes
AuditLog.Read.All,User.Read.All):
$cutoff = (Get-Date).AddDays(-90)
Get-MgUser -Filter "assignedLicenses/`$count ne 0" -ConsistencyLevel eventual -CountVariable
c -Property UserPrincipalName,SignInActivity -All | Where
{ $_.SignInActivity.LastSignInDateTime -lt $cutoff } | Select UserPrincipalName,
@{n='LastSignIn';e={$_.SignInActivity.LastSignInDateTime}}
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#42 Mailbox size vs license tier mismatch

HIGH FAIL

6 of 16 mailboxes need attention: 2 require SKU upgrade (Tier 1), 3 need archive enabled (Tier 2), 1 needs auto-expanding archive (Tier 3). See per-tier action list below.

```
Tier 1 — Cheapest fix: upgrade affected users from Microsoft 365 Business Premium
to M365 E3 (100 GB mailbox + 1.5 TB online archive). 2 users affected.
  • c***@e***.com  (48.0 GB / 50 GB cap)
  • s***@e***.com  (42.0 GB / 50 GB cap)

Tier 2 — Cheapest fix: enable Online Archive on the 3 affected mailboxes.
Exchange admin center → recipients → mailboxes → select user → Others → Manage
mailbox archive → On. Unlocks 1.5 TB archive storage per mailbox.
  • o***@e***.com  (87.0 GB)
  • h***@e***.com  (85.0 GB)
  • l***@e***.com  (82.0 GB)

Tier 3 — Cheapest fix: enable Auto-Expanding Archive via PowerShell (one-time
tenant config + per-mailbox flag). 1 user affected. Unlocks growth up to ~1.5 TB
additional per mailbox automatically.
  • a***@e***.com  (archive 1210.5 GB)
  Set-OrganizationConfig -AutoExpandingArchive
  Set-Mailbox -Identity a***@e***.com -AutoExpandingArchiveEnabled $true
```

✅ **Licensing:** Covered by your current licensing.

[See evidence]

#43 No redundant SKU stacking

LOW PASS

Configuration valid — no action required.

LOW V1.1 #44 Annual vs monthly commitment cost optimisation

7. Audit Logs & Incident Response

Checks #45–#50 · 6 total

#45 Unified audit log enabled

HIGH PASS

Configuration valid — no action required.

HIGH	V1.1	#46	Audit log retention policy ≥ 1 year
HIGH	V1.1	#47	Sign-in log retention adequate
HIGH	V1.1	#48	Mailbox audit search procedure documented
HIGH	V1.1	#49	Risk detection alert routing configured
HIGH	V1.1	#50	Periodic admin activity review scheduled

Evidence appendix

Raw API response excerpts captured during the audit, for review by your IT team. Only checks that returned data are listed; manual-review placeholders are documented inline in their section.

#01 Security Defaults OR Conditional Access enabled [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093088+00:00",
  "sample_field": "value-01"
}
```


#02 Legacy authentication blocked [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093113+00:00",
  "sample_field": "value-02"
}
```


#03 Break-glass (emergency) account exists [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093130+00:00",
  "sample_field": "value-03"
}
```


#06 Risky sign-in & risky user policies enabled [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093146+00:00",
  "sample_field": "value-06"
}
```


#08 Guest access governance [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093156+00:00",
  "sample_field": "value-08"
}
```

#09 Admin role count ≤ 5 [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093166+00:00",
  "sample_field": "value-09"
}
```


#10 Conditional Access policy hygiene [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093173+00:00",
  "sample_field": "value-10"
}
```


#11 SPF DNS record published with hard fail [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093180+00:00",
  "sample_field": "value-11"
}
```


#12 DKIM enabled for all sending domains [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093187+00:00",
  "sample_field": "value-12"
}
```


#13 DMARC record published (p=quarantine or p=reject) [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093193+00:00",
  "sample_field": "value-13"
}
```


#19 Default sharing capability not 'Anyone with the link' [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093214+00:00",
  "sample_field": "value-19"
}
```


#20 External sharing notifications routed to admin [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093221+00:00",
  "sample_field": "value-20"
}
```

#24 Anonymous link expiration ≤ 30 days [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093235+00:00",
  "sample_field": "value-24"
}
```


#30 Teams meeting recording auto-policy [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093275+00:00",
  "sample_field": "value-30"
}
```


#32 Device compliance enforced via Conditional Access [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093286+00:00",
  "sample_field": "value-32"
}
```


#33 Disk encryption required (BitLocker / FileVault) [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093292+00:00",
  "sample_field": "value-33"
}
```


#34 Compliance policy applied to all platforms [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093299+00:00",
  "sample_field": "value-34"
}
```


#35 Microsoft Defender for Endpoint deployed [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093305+00:00",
  "sample_field": "value-35"
}
```


#37 Intune device enrolment restrictions set [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093315+00:00",
  "sample_field": "value-37"
}
```

#40 Unassigned licenses ≤ 5% of total [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093327+00:00",
  "sample_field": "value-40"
}
```


#41 Inactive accounts retain assigned licenses [Back to summary]


```
{
  "checked_at": "2026-04-28T13:38:51.093334+00:00",
  "sample_field": "value-41"
}
```


#42 Mailbox size vs license tier mismatch [Back to summary]


```
{
  "auto_expand_detection": "manual_verification_required",
  "current_sku_distribution": {
    "Microsoft 365 Business Premium": 8,
    "Microsoft 365 E3": 6
  },
  "mailbox_total": 16,
  "recommended_actions": [
    {
      "action": "upgrade_sku",
      "from": "Microsoft 365 Business Premium",
      "tier": 1,
      "to": "Microsoft 365 E3",
      "users": [
        {
          "cap_gb": 50,
          "current_size_gb": 48.0,
          "upn": "c***@e***.com"
        },
        {
       ...
```


All data was read via the Microsoft Graph API using read-only Application permissions. No tenant data is retained after this report is generated. This report is informational and is not a substitute for a full security audit by a qualified consultant. Re-running this audit periodically is recommended; recommended cadence is monthly.