ASSESSMENT REPORT

Active Directory readiness assessment

Example Dental Group (sample)

Domain	**corp.example-dental.test**
Assessment date	**November 2, 2026**
Prepared by	**Your company name**
Contact	**help@your-msp.example | (555) 010-0100**
Readiness score	**10 / 100 · Significant work needed**

Confidential. This report describes security weaknesses in the named organization's systems. Share it only with people responsible for fixing them.

YOUR LOGO

EXECUTIVE SUMMARY

Where this domain stands



Significant work needed

This domain has 9 high-priority issues to fix before Microsoft's security changes take effect or before any move to cloud-only identity.

9	10	1	7
High priority: fix first	Medium: plan this quarter	Deadlines in the next 12 months	Systems that depend on the domain

What we found

HIGH **Domain controllers are past end of support.** The servers that control every sign-in no longer get security fixes. **F-01**

HIGH **Domain controllers are logging RC4 deprecation warnings (KDCSVC 201-209).** Windows itself is warning that some sign-ins will fail under Microsoft's new security rules. **F-02**

HIGH **Devices and apps bind to LDAP without signing, some in clear text.** Devices or applications send passwords across the network in readable form. **F-03**

HIGH **Computers on unsupported Windows versions.** Computers on unsupported Windows versions get no security fixes and will block later changes. **F-04**

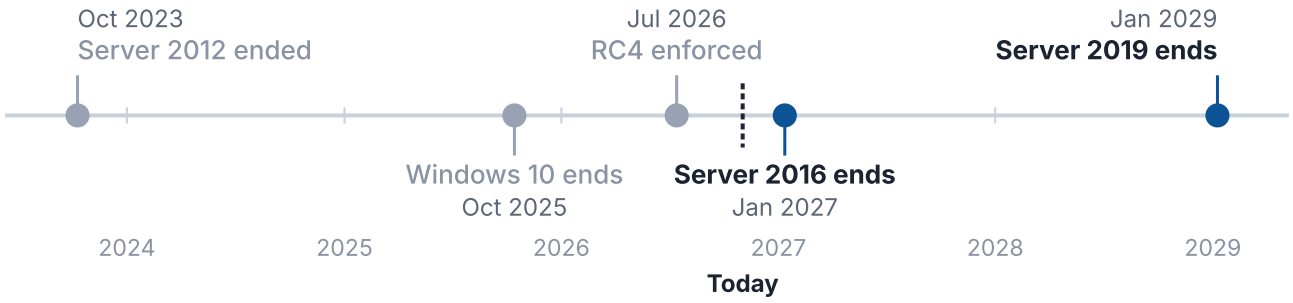
HIGH **NTLM version 1 is still in use.** A very old sign-in method is in use; it is easily cracked and already removed from new Windows. **F-05**

The decision in front of you

Your oldest domain controller lost security updates on **October 10, 2023**. Before spending on replacement servers, decide by **December 17, 2026** whether to rebuild them or move sign-in to Microsoft's cloud. The 7 items in phase 2 are what that decision depends on; phase 1 should start now either way.

TIMELINE AND ROADMAP

What is coming, and the order to tackle it



Also announced, no date yet: network NTLM disabled by default in the next major Windows Server release.

PHASE 1

Harden now

Needed whether the domain stays or goes. These break under Microsoft's security changes.

- **F-01** Domain controllers are past end of support
- **F-02** Domain controllers are logging RC4 deprecation warnings (KDCSVC 201-209)
- **F-03** Devices and apps bind to LDAP without signing, some in clear text
- **F-04** Computers on unsupported Windows versions
- **F-05** NTLM version 1 is still in use
- **F-06** Kerberos tickets are still issued with RC4
- **F-07** Accounts are explicitly set to RC4 without AES
- **F-08** Service accounts whose passwords predate AES keys
- **F-09** Windows 10 computers still joined to the domain
- **F-10** Computers whose support ends in the next 12 months
- **F-11** Enabled accounts whose passwords were set before AES keys existed
- **F-12** Domain controllers reach end of support within 15 months
- **F-13** Windows computers on a version that no longer gets security updates

PHASE 2

Replace what depends on it

Everything that signs in to the domain today. Each needs an owner and a replacement.

- **F-14** An internal certificate authority (AD CS) is in use
- **F-15** Non-Windows devices joined to the domain (Linux, NAS, appliances)
- **F-16** RADIUS servers (NPS) authenticate Wi-Fi or VPN against AD
- **F-17** Clients and apps still authenticate with NTLM
- **F-18** Service accounts that applications depend on
- **F-19** Group Policy objects to translate or drop
- **F-20** Printers are published from on-premises print servers

PHASE 3

Cut over and retire

Move identities and mail to the cloud, move devices, then retire the servers.

- **F-21** Exchange is (or was) installed in this AD forest
- **F-22** Stale accounts to clean up before migrating
- **F-23** The domain syncs to Entra ID (hybrid identity)

Effort on each finding is a rough guide for planning: **Hours**, **Days** or **Weeks** of technician time. Your IT provider will refine it.

SUPPORT COUNTDOWN

When each computer stops getting security updates

Support dates checked against Microsoft's lifecycle pages on October 30, 2026.

34	2	10	3	0
Past end of support	Ends within 90 days	Ends within 12 months	Ends in 1 to 3 years	More than 3 years left

12-month replacement plan

PRODUCT	COMPUTERS	UPDATES END	TIME LEFT	WHAT TO PLAN
Windows 7	1	2020-01-14	ended 6 years 9 months 19 days ago	Replace or disconnect from the network: no security updates of any kind.
Windows Server 2012 R2	1	2023-10-10	ended 3 years 23 days ago	Extended Security Updates (through Azure Arc) ended October 13, 2026; there is no year 4.
Windows 10 Pro 22H2	14	2025-10-14	ended 1 year 19 days ago	Paid Extended Security Updates available through October 12, 2027 (businesses can buy a third year to October 10, 2028).
Windows 11 Pro 23H2	2	2025-11-11	ended 11 months 22 days ago	Free feature update fixes this: install the latest Windows 11 version.
Windows 11 Pro 24H2	16	2026-10-13	ended 20 days ago	Free feature update fixes this: install the latest Windows 11 version.
Windows Server 2016	2	2027-01-12	2 months 10 days	Plan the upgrade or replacement now: Hyper-V Server 2016, WSUS on 2016 and .NET Framework 4.6.2 end the same day.
Windows 11 Pro 25H2	10	2027-10-12	11 months 10 days	Schedule the free feature update to the latest Windows 11 version before this date.

Every computer, soonest first

COMPUTER	ROLE	PRODUCT	UPDATES END	TIME LEFT
XRAY-PC	Workstation	Windows 7	2020-01-14	ended 6 years 9 months 19 days ago
DC02	Domain controller	Windows Server 2012 R2	2023-10-10	ended 3 years 23 days ago
HYG-01	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-02	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-03	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago

COMPUTER	ROLE	PRODUCT	UPDATES END	TIME LEFT
HYG-04	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-05	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-06	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-07	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-08	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-09	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-10	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-11	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-12	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-13	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
HYG-14	Workstation	Windows 10 Pro 22H2	2025-10-14	ended 1 year 19 days ago
BILLING-02	Workstation	Windows 11 Pro 23H2	2025-11-11	ended 11 months 22 days ago
DRSMITH-LT	Workstation	Windows 11 Pro 23H2	2025-11-11	ended 11 months 22 days ago
OP-01	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-02	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-03	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-04	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-05	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-06	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-07	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-08	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-09	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-10	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-11	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-12	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-13	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-14	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-15	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
OP-16	Workstation	Windows 11 Pro 24H2	2026-10-13	ended 20 days ago
DC01	Domain controller	Windows Server 2016	2027-01-12	2 months 10 days
FS01	Server	Windows Server 2016	2027-01-12	2 months 10 days
FRONT-01	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days
FRONT-02	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days
FRONT-03	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days
FRONT-04	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days
FRONT-05	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days
FRONT-06	Workstation	Windows 11 Pro 25H2	2027-10-12	11 months 10 days

COMPUTER	ROLE	PRODUCT	UPDATES END	TIME LEFT
FRONT-07	Workstation	Windows 11 Pro 25H2	2027-10-12	**11 months 10 days**
FRONT-08	Workstation	Windows 11 Pro 25H2	2027-10-12	**11 months 10 days**
FRONT-09	Workstation	Windows 11 Pro 25H2	2027-10-12	**11 months 10 days**

Showing the 45 soonest of 49 computers. The full list is in lifecycle.csv alongside this report.

Dates are the last Patch Tuesday with security updates, from Microsoft's lifecycle pages. Versions come from what each computer last reported to Active Directory.

FINDINGS

Detailed findings and actions

F-01 Domain controllers are past end of support

HIGH EFFORT: WEEKS

The servers that control every sign-in no longer get security fixes.

WHY IT MATTERS

No more security updates for the servers that hold every password in the domain. Cyber insurers and auditors flag this.

RECOMMENDED ACTION

Decide now: rebuild the DCs on Windows Server 2025, buy Extended Security Updates through Azure Arc as a short bridge, or retire AD entirely (phases 2 and 3).

EVIDENCE (1 FOUND)

DC02.corp.example-dental.test: Windows Server 2012 R2, support ends 2023-10-10

Cloud path: Microsoft Entra ID with Entra-joined devices, if phase 2 dependencies can be cleared.

Owner _____ Target date _____ Status (Harden now) _____

F-02 Domain controllers are logging RC4 deprecation warnings (KDCSVC 201-209)

HIGH EFFORT: DAYS

Windows itself is warning that some sign-ins will fail under Microsoft's new security rules.

WHY IT MATTERS

These are Microsoft's own warnings that something will break, or already has, under RC4 enforcement.

RECOMMENDED ACTION

Fix each account or setting named in the events; event 205 means DefaultDomainSupportedEncTypes still allows RC4.

EVIDENCE (1 EVENT)

account svc_imaging - last seen 2026-10-15 (1 event)

Owner _____ Target date _____ Status (Harden now) _____

F-03 Devices and apps bind to LDAP without signing, some in clear text

HIGH EFFORT: DAYS

Devices or applications send passwords across the network in readable form.

WHY IT MATTERS

Simple binds send passwords in clear text. Each client here is also an app that talks to AD directly, so it blocks a move to cloud-only.

RECOMMENDED ACTION

Switch each client to LDAPS (636) or signed binds, then require LDAP signing and channel binding on the DCs. Typical culprits: copiers scanning to email, firewalls, VPNs, Wi-Fi controllers, line-of-business apps.

EVIDENCE (1 EVENT)

account EXDENTAL\ldap-firewall from 10.0.0.90 - simple bind (clear text) - last seen 2026-10-14 (1 event)

Cloud path: Modern auth (SAML/OIDC) via Entra ID, or Microsoft Entra Domain Services as a bridge for apps that can only speak LDAP.

Owner _____ Target date _____ Status (Harden now) _____

F-04 Computers on unsupported Windows versions

HIGH | EFFORT: WEEKS

Computers on unsupported Windows versions get no security fixes and will block later changes.

WHY IT MATTERS

No security updates; most also can't do modern Kerberos or join Entra ID.

RECOMMENDED ACTION

Replace or isolate them before tightening RC4, NTLM or LDAP settings, or they will stop working.

EVIDENCE (2 FOUND)

XRAY-PC: Windows 7 Professional
DC02: Windows Server 2012 R2 Standard

Cloud path: Windows 11 devices joined to Entra ID and managed by Intune.

Owner _____ Target date _____ Status (Harden now) _____

F-05 NTLM version 1 is still in use

HIGH | EFFORT: DAYS

A very old sign-in method is in use; it is easily cracked and already removed from new Windows.

WHY IT MATTERS

NTLMv1 is removed from Windows 11 24H2 and Server 2025 and can be cracked quickly. Anything listed here breaks on those versions.

RECOMMENDED ACTION

Find the device or app on each listed client, update or replace it, then set LAN Manager authentication level to "Send NTLMv2 response only. Refuse LM & NTLM".

EVIDENCE (1 EVENT)

account EXDENTAL\xrayuser from XRAY-PC (10.0.0.77) - last seen 2026-10-13 (1 event)

Owner _____ Target date _____ Status (Harden now) _____

F-06 Kerberos tickets are still issued with RC4

HIGH | EFFORT: DAYS

Some sign-ins still use an old encryption method Microsoft is switching off; those may stop working.

WHY IT MATTERS

Microsoft moved RC4 to enforcement in 2026; the July 2026 update removed the rollback switch. These accounts or devices can fail to sign in after updates, and RC4 tickets are easy to crack offline.

RECOMMENDED ACTION

Reset passwords on the listed service accounts so they get AES keys, set msDS-SupportedEncryptionTypes to AES, and update keytabs or krb5.conf on Linux, NAS and Java systems. Re-run the scan until this list is empty.

EVIDENCE (1 EVENT)

account frontdesk1@CORP.EXAMPLE-DENTAL.TEST from 10.0.0.41 to svc_imaging - last seen 2026-10-10 (1 event)

Cloud path: Not needed once fixed; Entra ID does not use RC4.

Owner _____ Target date _____ Status (Harden now) _____

F-07 Accounts are explicitly set to RC4 without AES

HIGH | EFFORT: HOURS

Some accounts are locked to an outdated encryption method and are likely to break.

WHY IT MATTERS

An explicit RC4-only setting keeps RC4 alive after enforcement and marks something that probably can't do AES.

RECOMMENDED ACTION

Confirm what uses each account, test AES, then set msDS-SupportedEncryptionTypes to 0x18 (AES128 and AES256).

EVIDENCE (2 FOUND)

- svc_imaging (user): RC4-HMAC
- NAS01$ (computer): RC4-HMAC

Owner _____ Target date _____ Status (Harden now) _____

F-08 Service accounts whose passwords predate AES keys

HIGH | EFFORT: DAYS

Accounts that run business applications have passwords too old for modern encryption.

WHY IT MATTERS

Passwords set before the domain reached the 2008 functional level have no AES keys, so these accounts can only use RC4 and are the most likely to break.

RECOMMENDED ACTION

Reset each password twice (with the application owner present), then confirm the app still signs in.

EVIDENCE (1 FOUND)

- svc_sql, password last set 2009-06-14

Cloud path: Long term: a managed identity, app registration or gMSA instead of a password account.

Owner _____ Target date _____ Status (Harden now) _____

F-09 Windows 10 computers still joined to the domain

MEDIUM | EFFORT: WEEKS

Windows 10 is out of support; these computers need replacing or paid extended updates.

WHY IT MATTERS

Windows 10 support ended October 14, 2025; continuing updates require paid Extended Security Updates.

RECOMMENDED ACTION

Fold their replacement into the device plan: new or upgraded devices go straight to Entra join with Autopilot.

Cloud path: Windows 11, Entra-joined, Intune-managed.

Owner _____ Target date _____ Status (Harden now) _____

F-10 Computers whose support ends in the next 12 months

MEDIUM EFFORT: WEEKS

Some computers stop getting security fixes within a year; they belong in this year's budget.

WHY IT MATTERS

Each line is a dated budget item. Replacing or upgrading on schedule is cheaper than an emergency project, paid Extended Security Updates, or a failed insurance questionnaire.

RECOMMENDED ACTION

Put each product on the replacement plan with an owner and a month: servers to Windows Server 2025 (or retire them into Microsoft 365 or Azure), Windows 11 computers to the latest feature update, long-term servicing devices to Windows 11 LTSC 2024.

EVIDENCE (11 FOUND)

Windows Server 2016: 2 months 10 days (2027-01-12) - FS01
Windows 11 Pro 25H2: 11 months 10 days (2027-10-12) - FRONT-01, FRONT-02, FRONT-03, FRONT-04, FRONT-05, FRONT-06 and 4 more

Cloud path: Servers that only host files or line-of-business apps may move to SharePoint, Azure Files or the vendor's cloud version instead of being rebuilt.

Owner _____ Target date _____ Status (Harden now) _____

F-11 Enabled accounts whose passwords were set before AES keys existed

MEDIUM EFFORT: HOURS

A few accounts have passwords older than the domain's modern encryption and should be changed.

WHY IT MATTERS

These accounts can only use RC4 until their password is changed. Usually they are long-forgotten accounts; in a newly built domain the built-in Administrator also appears, because its password was carried over from before the domain existed.

RECOMMENDED ACTION

Disable the ones nobody uses; change the password on the rest (any change creates the AES keys).

EVIDENCE (1 FOUND)

frontdesk2, password last set 2010-11-03
This domain could first create AES keys on 2011-03-02; passwords set before then have none.

Owner _____ Target date _____ Status (Harden now) _____

F-12 Domain controllers reach end of support within 15 months

MEDIUM EFFORT: WEEKS

The servers that control every sign-in stop getting security fixes soon, so a replacement decision is due.

WHY IT MATTERS

A server refresh is coming either way. Pricing it against retiring AD now avoids buying hardware and licences twice.

RECOMMENDED ACTION

Use this report to choose between a like-for-like refresh and a move to cloud-only before the date.

EVIDENCE (1 FOUND)

DC01.corp.example-dental.test: Windows Server 2016, support ends 2027-01-12

Cloud path: Microsoft Entra ID.

Owner _____ Target date _____ Status (Harden now) _____

F-13 Windows computers on a version that no longer gets security updates

MEDIUM EFFORT: DAYS

Some computers run a Windows version that no longer gets security fixes; a free update brings them current.

WHY IT MATTERS

Windows 11 versions stop getting security updates 24 months after release (Home and Pro) or 36 months (Enterprise and Education). These computers are patched in name only.

RECOMMENDED ACTION

Windows 11: push the latest feature update (free) through Windows Update for Business, Intune or your RMM, and check nothing is pinning the old version (TargetReleaseVersion policy). Long-term servicing editions: replace or move to Windows 11 LTSC 2024.

EVIDENCE (18 FOUND)

Windows 11 Pro 23H2: ended 11 months 22 days ago (2025-11-11) - BILLING-02, DRSMITH-LT
Windows 11 Pro 24H2: ended 20 days ago (2026-10-13) - OP-01, OP-02, OP-03, OP-04, OP-05, OP-06 and 10 more

Cloud path: Windows Autopatch or Intune feature-update policies keep versions current automatically.

Owner _____ Target date _____ Status (Harden now) _____

F-14 An internal certificate authority (AD CS) is in use

HIGH EFFORT: WEEKS

An internal certificate system supports Wi-Fi, VPN or devices and needs a replacement plan.

WHY IT MATTERS

Wi-Fi (802.1X), VPN and device certificates often depend on it, and a CA on an end-of-support server is a top attack target.

RECOMMENDED ACTION

List what each certificate template is used for, migrate the CA off old servers, and plan its replacement before retiring AD.

EVIDENCE (1 FOUND)

EXDENTAL-CA on DC01.corp.example-dental.test

Cloud path: Microsoft Intune Cloud PKI or a hosted PKI service.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-15 Non-Windows devices joined to the domain (Linux, NAS, appliances)

MEDIUM EFFORT: DAYS

Non-Windows devices (storage, Linux, appliances) depend on the domain and need a new home.

WHY IT MATTERS

These rely on Kerberos or LDAP from AD and are often the ones still using RC4. None of them can join Entra ID directly.

RECOMMENDED ACTION

For each, find what it uses AD for (file sharing permissions, admin sign-in, LDAP lookups) and choose a replacement before retiring the DC.

EVIDENCE (2 FOUND)

NAS01: operating system not recorded
XRAYLNX: Linux

Cloud path: Azure Files or SharePoint for NAS data; Entra Domain Services or the vendor's SAML/OIDC option for appliances.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-16 RADIUS servers (NPS) authenticate Wi-Fi or VPN against AD

MEDIUM | EFFORT: DAYS

Wi-Fi or VPN sign-in runs through the domain and stops when it goes.

WHY IT MATTERS

Wi-Fi and VPN sign-in stop working when the DC goes.

RECOMMENDED ACTION

Inventory which networks and VPNs use each NPS server and move them to a cloud RADIUS service or certificate-based Wi-Fi.

EVIDENCE (1 FOUND)

DC01

Cloud path: Cloud RADIUS with Entra ID, or Entra Private Access in place of the VPN.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-17 Clients and apps still authenticate with NTLM

MEDIUM | EFFORT: DAYS

Devices still use a sign-in method Microsoft plans to switch off by default.

WHY IT MATTERS

Microsoft will disable network NTLM by default in the next major Windows Server release. Many NTLM users are also apps tied to on-premises AD.

RECOMMENDED ACTION

Work through the list by client: connect by name not IP so Kerberos is used (Remote Desktop or file shares opened by IP address are a common source), fix missing SPNs, and update or replace apps hard-coded to NTLM.

EVIDENCE (1 EVENT)

account scanner from FRONTDESK-MFP - last seen 2026-10-12 (1 credential check)

Cloud path: Kerberos now; Entra ID sign-in for apps that move to the cloud.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-18 Service accounts that applications depend on

MEDIUM | EFFORT: WEEKS

Business applications sign in to the domain and must be moved before it can be retired.

WHY IT MATTERS

Each one is an application or service that authenticates against AD. Guides on retiring AD call these the most common reason projects stall.

RECOMMENDED ACTION

Give every account an owner, the app it serves, and a target: modernize, move to a managed identity, keep behind Entra Domain Services, or delete.

EVIDENCE (3 FOUND)

svc_sql: MSSQLSvc/SQL01.corp.example-dental.test:1433

svc_imaging: HTTP/imaging.corp.example-dental.test

svc_backup: HOST/backup01

Cloud path: Managed identities or app registrations in Entra ID; Entra Domain Services for apps that can't change.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-19 Group Policy objects to translate or drop

LOW | EFFORT: DAYS

Computer settings are pushed by Group Policy and must be rebuilt for cloud management.

WHY IT MATTERS

Entra-joined devices don't receive Group Policy. Copying every GPO recreates the sprawl in Intune.

RECOMMENDED ACTION

Delete unlinked GPOs, run Intune Group Policy analytics on the rest, and rebuild only what is still needed as Intune profiles.

EVIDENCE (23 FOUND)

23 GPOs, 6 not linked anywhere

Cloud path: Intune configuration profiles and security baselines.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-20 Printers are published from on-premises print servers

LOW | EFFORT: DAYS

Printing runs through on-site print servers that need a cloud replacement.

WHY IT MATTERS

Entra-joined devices can't use AD-published printers the same way, and print servers are often old.

RECOMMENDED ACTION

Move queues to a cloud print service; check which copiers also scan to SMB shares or use LDAP address books.

EVIDENCE (2 FOUND)

Print server: PRINT01.corp.example-dental.test

Cloud path: Universal Print.

Owner _____ Target date _____ Status (Replace dependencies) _____

F-21 Exchange is (or was) installed in this AD forest

MEDIUM | EFFORT: WEEKS

Mailbox settings are still managed from the on-site domain and must move first.

WHY IT MATTERS

Mail attributes for synced users are managed from AD. Uninstalling the last Exchange server the wrong way breaks recipient management.

RECOMMENDED ACTION

Make mailboxes cloud-managed (IsExchangeCloudManaged) before removing sync. Shut down, don't uninstall, the last Exchange server until then.

EVIDENCE (1 FOUND)

EX2016 Version 15.1 (Build 30225.48)

Cloud path: Exchange Online with cloud-managed Exchange attributes.

Owner _____ Target date _____ Status (Cut over and retire) _____

F-22 Stale accounts to clean up before migrating

LOW | EFFORT: HOURS

Unused accounts should be removed before anything is migrated.

WHY IT MATTERS

Migrating dead accounts costs licences and time and leaves easy targets.

RECOMMENDED ACTION

Disable, wait 30 days, then delete. Migrate only active accounts.

EVIDENCE (15 FOUND)

9 enabled users and 6 enabled computers with no logon in 90 days

Owner _____ Target date _____ Status (Cut over and retire) _____

F-23 The domain syncs to Entra ID (hybrid identity)

INFO | EFFORT: DAYS

Users already exist in Microsoft's cloud directory, which shortens the move.

WHY IT MATTERS

Good news: users already exist in Entra ID. To retire AD, their source of authority must move to the cloud first. Seamless SSO's computer account also commonly uses RC4.

RECOMMENDED ACTION

Convert synced users and groups to cloud management (generally available since January 2026 for users), then remove sync. Move devices to Entra join and retire Seamless SSO.

EVIDENCE (1 FOUND)

Sync account: MSOL_0a1b2c3d4e5f
Seamless SSO computer account AZUREADSSOACC is present

Cloud path: Cloud-managed users and groups in Entra ID.

Owner _____ Target date _____ Status (Cut over and retire) _____

APPENDIX

Environment and method

Environment

Domain / NetBIOS name	corp.example-dental.test / EXDENTAL
Functional level	Windows2012R2Domain
Users (enabled of total)	48 of 61
Computers (enabled of total)	52 of 58
Service accounts	3
Group Policy objects	23
Sites	1

Computers by operating system

Windows 11 Pro	28
Windows 10 Pro	14
Windows Server 2019 Standard	3
Windows Server 2016 Standard	2
Windows 7 Professional	1
(blank)	1
Windows Server 2012 R2 Standard	1
Linux	1

Domain controllers

SERVER	OPERATING SYSTEM	SITE	SUPPORT ENDS
DC01.corp.example-dental.test	Windows Server 2016 Standard	Default-First-Site-Name	2027-01-12
DC02.corp.example-dental.test	Windows Server 2012 R2 Standard	Default-First-Site-Name	2023-10-10

Scan coverage

Domain controller event logs were read for the last 14 days. Only events still held in each log can be found.

SERVER	LOG OR CHECK	RESULT
DC01	Security (log window)	Oldest event 2026-10-19 08:00
DC01	Security RC4 tickets	4 matched

How this assessment was done

Read-only queries of Active Directory and of the domain controllers' security, directory service and system event logs. Nothing was changed. Findings reflect what was visible during the scan

Glossary

Active Directory (AD)
The on-site directory that controls sign-in to Windows computers, file shares and many applications.

window; systems that did not sign in during that window will not appear, so a repeat scan before any cutover is recommended.

Produced with AD Exit Planner 0.3.0.

Severity: **High** = breaks or exposes the business under current or scheduled changes; **Medium** = must be planned before a change; **Low** = housekeeping.

Microsoft Entra ID
Microsoft's cloud directory, used by Microsoft 365. Can replace AD for most small businesses.

RC4, AES
Encryption methods for sign-in tickets. RC4 is outdated and being switched off; AES is the replacement.

NTLM
An older Windows sign-in method. Microsoft is phasing it out in favor of Kerberos.

LDAP signing
Protection for the way devices and applications look up users. Without it, passwords can cross the network readable.