Paid Credential Exposure Findings Report

This is a mockup that demonstrates the format of a paid credential exposure findings report. Healthviro is a fictional organization.

Executive Summary & Opinion & Advisory - Healthviro

Assessment Snapshot

- Overall result: Password security was materially weak, with 1,465 of 4,748 enabled Active Directory accounts, 30.9%, compromised during testing.
- Main exposure: Password reuse was widespread across active and operational accounts, including one shared password used by 530 enabled accounts.
- Higher-risk impact: 160 higher-impact accounts were compromised, including service and privileged operational accounts, and 953 compromised accounts were also non-expiring.
- Business implication: If password data were obtained by an attacker, the findings indicate a credible path to broader unauthorized access, operational disruption, longer persistence, and more difficult containment.
- Balancing point: No Domain Admin passwords were cracked, but the overall result still points to a systemic credential-governance and enforcement problem requiring prompt action.

Executive Summary

Scapien performed a password security assessment of a representative Active Directory environment using synthetic assessment data. The assessment was designed to simulate the kinds of methods a real attacker would use if password data were obtained and then tested for practical abuse. In plain terms, the goal was to measure how successful an attacker could be in turning compromised passwords into real access, wider movement, and longer-term footholds inside the environment.

This section summarizes the most important results of that work. The report includes detailed findings, supporting evidence, remediation guidance, and advisory context for the security risks identified during the assessment. Scapien's focus was not just on whether passwords could be cracked, but on what those results would mean in a real compromise scenario, including whether an attacker could use them to move further, reach more valuable accounts, or maintain access for longer than expected.

The overall result was materially weak. The strongest pattern was not a single isolated flaw, but a broader breakdown in credential discipline across active accounts, shared-function accounts, and operational workflows. Of the 4,748 enabled Active Directory user accounts in scope, 1,465, or 30.9%, were compromised during testing. That is large enough to indicate a systemic issue rather than a small pocket of weak user behavior.

The main themes were password reuse, weak password construction, non-expiring credentials, and a policy-to-enforcement gap. These issues appear to be built into day-to-day operations, especially across service-style accounts, shared-function accounts, kiosk and exam workflows, and other long-lived operational identities. The result is an environment where a real attacker would have multiple practical ways to turn stolen password data into broader access.

There were, however, meaningful positives. No Domain Admin passwords were cracked. No enabled accounts had blank passwords. Password complexity, lockout settings, and a stronger fine-grained password policy were present in the environment. Those controls helped prevent an even worse outcome. The problem is that the live password results did not reflect the stated policy intent, which

points to an enforcement and operational-discipline problem rather than a total absence of control design.

Business Risk

The business risk here is straightforward: if an attacker obtained password data from this sample environment, there is a high likelihood they could convert that data into usable access across a meaningful share of the organization, including operational and higher-impact accounts. The findings show both scale and concentration, which increases the likelihood of disruption, unauthorized access, prolonged exposure, and more expensive containment.

- 1,465 enabled accounts, or 30.9%, were compromised, meaning nearly one-third of active user accounts could potentially be abused by an attacker.
- 1,173 compromised accounts shared passwords, so one cracked password could open many accounts at once.
- One repeated password was used by 530 enabled accounts, creating a very large blast radius from a single compromise.
- 160 higher-impact accounts were compromised, including service or shared-function accounts and privileged operational accounts.
- 953 compromised accounts were also non-expiring, allowing stolen access to remain useful until someone resets it.
- 1,163 compromised accounts were below the current 14-character baseline, showing the problem is not just reuse but weak password quality at scale.

As a result, a realistic compromise could allow an attacker to expand access quickly, move through shared operational workflows, abuse service-style identities that support daily functions, and maintain access for longer than management would reasonably expect. It would also make containment more expensive and more difficult, because resetting one user or one system would not remove the wider exposure where the same passwords, similar patterns, or non-expiring credentials remain in place. Depending on how these accounts intersect with regulated and sensitive workflows, the findings may also create audit and compliance pressure if the organization cannot demonstrate timely remediation and stronger ongoing control discipline.

Key Assessment Points & Recommendations

This assessment used synthetic Active Directory assessment data and analyzed it using attacker-style cracking and validation methods to determine both password weakness and likely business impact if those passwords were abused in a real compromise. That allowed Scapien to evaluate not just which passwords failed, but how those failures clustered across user populations, operational accounts, and higher-impact identities.

The detailed findings document the affected accounts, evidence, scoring rationale, and remediation guidance for each security risk. They also show why this result should be treated as an operational work program rather than a one-time technical cleanup. In this case, the findings support a phased response, beginning with the most dangerous credential concentrations and the smaller high-impact account subset, then moving into the broader reset and governance work needed to prevent recurrence.

Scapien's Customer Remediation System (CRS) should be used as the central mechanism for managing this work. CRS allows the organization to track what was remediated, when it was remediated, who owned the work, and what was validated and closed. That audit trail is valuable not only for day-to-day risk reduction, but also for cybersecurity maturity, SOC 2 and audit risk reporting, and demonstrating responsible action if the organization later faces legal, regulatory, or third-party scrutiny.

Because several findings relate to shared credential patterns, common operational account types, and repeatable governance failures, parts of the remediation can be standardized and applied broadly. The first wave is already clearly defined by the report data: the 160-account high-impact subset and the highest-volume repeated passwords offer the cleanest initial package for rapid risk reduction. From there, the broader reset and policy-enforcement effort can be sequenced in a more controlled way. Scapien recommends prompt action, starting with the highest-risk repeated passwords and the 160-account high-impact subset, then extending into the broader password reset, exception reduction, and policy-enforcement work needed to materially reduce attacker success rates.

Opinion and Advisory

Observations

Healthviro's results in this assessment were weak, and weaker than would be expected in a well-governed mid-market environment with a stated 14-character baseline and a fine-grained 16-character policy already in place. The core issue is not simply that some users chose poor passwords. The stronger conclusion is that credential weakness has become embedded in operating practice across shared-function accounts, service-style accounts, and long-lived operational workflows. In other words, the control design exists in part, but the live outcome is materially below the standard the organization appears to believe it is enforcing.

That said, the result is not equivalent to total control failure. Healthviro avoided the most serious immediate scenario because no Domain Admin passwords were cracked. Blank passwords were not present. Complexity, lockout controls, and stronger policy intent were visible in the environment. Those positives matter, because they show the organization has some sound baseline decisions in place. The problem is that those controls are being undermined by exception handling, weak lifecycle management, and operational convenience. Without intervention, this is likely to persist, because the findings point to a recurring discipline and governance problem rather than a one-off technical miss.

Recommendations

The right response is to treat this as both a remediation problem and a control-governance problem. The immediate task is to remove the most dangerous live exposure, especially where password reuse, higher-impact accounts, and non-expiring credentials overlap. The broader task is to bring operating practice back into line with policy intent, reduce the number of fragile exceptions the environment depends on, and establish clearer ownership over service, shared-function, and other non-human identities. In practical terms, Healthviro should use the short-term plan to cut attacker leverage quickly, then use the longer-term plan to fix the operating model that allowed these weaknesses to accumulate.

Short-term Tactical Plan (7–45 days)

- Reset the highest-risk credential concentrations first, starting with the top repeated passwords and the 160 high-impact compromised accounts that offer the greatest operational leverage to an attacker.
- Reset all compromised non-expiring accounts and assign named ownership to service, shared-function, and other long-lived operational identities before those accounts are allowed to remain in service.
- Validate the first remediation wave quickly through re-checking, so management knows the most dangerous exposure has actually been removed rather than merely planned for removal.

Long-term Strategic Plan (45 days–12 months)

1. Redesign service-account and shared-function account management so critical operational identities use unique managed credentials and no longer depend on shared passwords or convenience-based practices.

2. Align password policy with real enforcement by tightening exception handling, verifying fine-grained policy application, and ensuring resets, onboarding, and lifecycle events cannot bypass the intended standard.
3. Establish formal ownership and review processes for non-human, kiosk, exam, template-derived, and other operational accounts that have historically been allowed to drift outside normal control discipline.
4. Implement password screening and pattern-blocking controls to reduce branded, predictable, and attacker-friendly password construction across the environment.
5. Schedule periodic validation of password hygiene and exception populations so management can detect drift early rather than relearning the problem during the next assessment.

Conclusion

If Healthviro follows this advisory, the organization should be able to move from a materially weak credential posture to a far more controlled and defensible state, with lower attacker success rates, reduced blast radius, and stronger confidence that policy intent is actually reflected in day-to-day operations. Using CRS alongside the remediation program will also improve cybersecurity maturity over time by giving the organization disciplined tracking, evidence retention, audit support, stronger accountability, and a verifiable record of what was fixed, when it was fixed, and how closure was validated.

Findings Report

Assessment Scope and Result Summary

- Total number of accounts provided by the organization: 22,258
- Total number of enabled Active Directory user accounts in scope: 4,748
- Total number of unique enabled user accounts compromised: 1,465
- Percentage of enabled user accounts compromised: 30.9%
- Privileged accounts compromised: 8 of 1,465 (0.5%)
- Service/domain/operational accounts compromised: 153 of 1,465 (10.4%)
- Percentage of compromised enabled accounts that had no password: 0 of 1,465 (0.0%)
- Percentage of compromised enabled accounts that shared the same password with at least one other enabled account: 1,173 of 1,465 (80.1%)

Findings

1. Category: Weak Credentials —— Password Reuse Across Enabled Accounts

Security Risk Score: 9.3/10

Risk
If many enabled accounts use the same password, one compromise can expose many accounts at once. That lets an attacker move faster, expand access quickly, and make containment harder. It also raises the chance of business disruption because resetting one account may not remove the wider exposure.

Issue
Password reuse breaks account separation.
• One cracked or obtained password can unlock multiple enabled accounts
• Attackers do not need to compromise each account one by one
• Shared passwords increase blast radius and complicate cleanup
• The risk is worse when reuse reaches service, shared-function, or operational accounts

Susceptibility
This is easy to exploit once an attacker obtains any valid reused password through standard attacker password cracking techniques, phishing, credential capture, or replay. The more widely that password is reused, the faster an attacker can move across the environment.

Organization Notes
This was the strongest issue found. Of the 1,465 enabled user accounts whose passwords were cracked, 1,173 accounts, or 80.1%, were using a password shared by at least one other enabled account. The largest repeated values were Hvc12345 used by 530 enabled accounts, Hvc123456789 used by 238, Hvc12345! used by 133, Healthviro12345678 used by 123 across two repeated-password clusters, HVC@2021 used by 50, and Hvc54321 used by 45. Reuse was not limited to low-value users. It appeared across service-style accounts, shared-function accounts, shared inbox accounts, kiosk and exam accounts, and named user accounts. This is an operational password-management problem, not a small number of isolated weak choices.

Scoring

- Final Adjusted Score: 9.3
- CVSS 4.0 Environmental Score: 8.1
- BTE Adjustment: +1.2

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- Proven exploitability: one cracked password often applied to many enabled accounts
- High exposure: reuse crossed service, operational, and regular-user populations
- Large blast radius: attacker movement becomes much faster once one shared password is known
- High operational consequence: multiple repeated-password clusters sat inside daily workflows

Targets
Target count: 1,173 enabled accounts

Highly privileged:
Privileged_ops_001, healthviro.example, 16; privileged_ops_002, healthviro.example, 8; privileged_ops_003, healthviro.example, 10

Service/domain/operational accounts:
medicalrecords_report2, healthviro.example, 8; familymedicine_schedules, healthviro.example, 9; helpdesk_inbox, healthviro.example, 9; clinic_generalbox, healthviro.example, 8; hr_inbox, healthviro.example, 9; internal_news, healthviro.example, 16; clinical_triage_1, healthviro.example, 8; dental_scan_queue, healthviro.example, 9; clinic_inbox, healthviro.example, 8; scanner_ops, corp.healthviro.example, 8; Healthviroconnect, healthviro.example, 8; Healthviromembercommun, healthviro.example, 8; Healthviroroc, healthviro.example, 12; hvcbehavioralhealth, healthviro.example, 15; mailflow, healthviro.example, 8; mycharthelp, healthviro.example, 8; obgynurgentline, healthviro.example, 17; payroll_inbox, healthviro.example, 9; pharmacyeligibility, healthviro.example, 8; pharmacypurchasing, healthviro.example, 12; preventioniscare, healthviro.example, 8; restrictedencounter, healthviro.example, 8; schoolhealth, healthviro.example, 8; ssiforms, healthviro.example, 8; urgentcare_inbox, healthviro.example, 9; streetmedreferrals, healthviro.example, 8; tobaccotreatment, healthviro.example, 8; compliance_inbox, healthviro.example, 9; eligibility_inbox, healthviro.example, 9; wellnesscenter, healthviro.example, 8; media_training, corp.healthviro.example, 10; conference_ops, healthviro.example, 10

High-data-access users:
user_data_001, healthviro.example, 14; user_data_002, healthviro.example, 17; user_data_003, healthviro.example, 14; user_data_004, healthviro.example, 16; user_data_005, healthviro.example, 15; user_data_006, healthviro.example, 13; user_data_007, healthviro.example, 12; user_data_008, healthviro.example, 12; user_data_009, healthviro.example, 16; user_data_010, healthviro.example, 14; user_data_011, healthviro.example, 16; user_data_012, healthviro.example, 9; user_data_013, healthviro.example, 14; user_data_014, healthviro.example, 13; user_data_015, healthviro.example, 14; user_data_016, healthviro.example, 12; user_data_017, healthviro.example, 15; user_data_018, healthviro.example, 11

Regular users:
Large reused-password groups existed across ClinicExam01-ClinicExam10, AccessCheck01-AccessCheck08, ProviderExam01-ProviderExam10, OpsExam01-OpsExam17, training01-training12, DentalOps01-DentalOps14, intakecheck01-intakecheck04, wellnesscheck01-wellnesscheck02, wardA_exam01-wardA_exam10, wardB_exam01-wardB_exam09, wardC_exam01-wardC_exam09, plus multiple shared inbox, shared mailbox, and template-derived operational identities.

Organization Notes
```
The repeated-password problem is tied to how these accounts are being managed. The biggest
clusters sat in exam, kiosk, dental, training, shared inbox, and shared-function accounts.
That means this is also an account-lifecycle and operations problem. The fastest first move
is to reset the highest-volume repeated passwords and include the named service and shared-
function accounts in that same change wave.
```

Remediation
Description
Remove shared passwords and replace them with unique credentials.

Minimum role required
Active Directory engineer; senior identity or platform owner for service-account redesign.

Up to 3 remediation options

1. Preferred: Reset all reused passwords and move non-human accounts to unique managed credentials.
2. Reset reused passwords first, then redesign service-account handling in phases.
3. Lock down the highest-risk reused accounts first, then reset by business unit.

Preferred option and why

Option 1 is preferred because it fixes the root cause.

Remediation steps

1. Find every enabled account using a duplicated password.
2. Reset the highest-volume repeated passwords first.
3. Reset named service accounts and privileged operational accounts in the same change window.
4. Replace shared service credentials with unique, long credentials under managed control.
5. Remove password sharing from kiosk, exam, template, and shared operational workflows.
6. Add detection to flag future password reuse.

Quick self-check

- No enabled accounts still use the top repeated passwords
- Service accounts no longer share passwords with any other account
- Duplicate-password groups drop sharply after recheck

Remediation references

- NIST SP 800-63B
- MITRE ATT&CK: T1110.002, T1078, T1078.002, T1110.003

Remediation Note

For this sample environment, the fastest risk reduction comes from resetting the seven highest-volume repeated passwords first and including the named service-account and shared-function population in that first action.

Effort Estimate

High (>1 Day)

Evidence

- Hvc12345 — 530 enabled accounts
- Hvc123456789 — 238
- Hvc12345! — 133
- Healthviro12345678 — 123 across two repeated-password clusters
- HVC@2021 — 50
- Hvc54321 — 45

Known References

- MITRE ATT&CK: T1110.002 Password Cracking; T1078 Valid Accounts; T1078.002 Domain Accounts; T1110.003 Password Spraying
- NIST SP 800-63B password guidance

2. Category: Privilege Exposure — Cracked Passwords on Privileged, Service, and Shared-Function Accounts

Security Risk Score: 9.2/10

Risk
When passwords are cracked on privileged, service, or shared-function accounts, the impact can be much higher than for a normal user compromise. These accounts often touch more systems, more workflows, or more sensitive data. That raises both business and operational risk.

Issue
Service and privileged operational accounts often have broader reach than standard users.

- If those passwords are cracked, an attacker can move faster
- Shared-function accounts are often weakly owned and rarely reviewed
- Even without Domain Admin access, these accounts can provide meaningful leverage

Susceptibility
This becomes easy to exploit once an attacker has a cracked password for a high-value account. The risk rises if the account is shared, non-expiring, tied to infrastructure, or used across multiple workflows.

Organization Notes
This sample environment had 160 high-impact enabled accounts in the cracked population: 153 service, domain, shared-function, or similar operational accounts, plus 8 adminCount=1 privileged operational accounts. No Domain Admin passwords were cracked, which is positive, but this still matters because these accounts are the ones most likely to help an attacker move faster or create disruption. The cracked high-impact set included shared inbox accounts, shared-function accounts, IT-related service accounts, operational support accounts, operational mailbox-style accounts, and several identities used in daily workflows

Scoring

- Final Adjusted Score: 9.2
- CVSS 4.0 Environmental Score: 8.3
- BTE Adjustment: +0.9

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- High business impact: affected accounts support shared functions and operational workflows
- Higher attacker value: these accounts offer more leverage than a standard user
- Proven exploitability: passwords on these accounts were already cracked
- Operational spread: affected accounts support multiple business functions and service paths

Targets
Target count: 160 enabled accounts

Highly privileged:
Privileged_ops_001, healthviro.example, 16; privileged_ops_002, healthviro.example, 8; privileged_ops_003, healthviro.example, 10

Service/domain/operational accounts:
clinical_credentialing_inbox, healthviro.example, 9; neonatal_operations_inbox, healthviro.example, 9; adm_fellowship_ops, healthviro.example, 8; admin_patientservices_inbox, healthviro.example, 9; emergencykits, healthviro.example, 12; accounts_payable, healthviro.example, 6; wellness_ops, healthviro.example, 8; badge_inventory, healthviro.example, 9; benefits, healthviro.example, 8; regionalclinic_general_inbox, healthviro.example, 9; regionalclinic_admin_inbox, healthviro.example, 9; behavioralhealth_workgroup, healthviro.example, 8; billing, healthviro.example, 8; clinicalops_group, healthviro.example, 8; patientservice_inbox, healthviro.example, 8; pediatric_lab, healthviro.example, 12; preadmission_lab, healthviro.example, 12; carecoordination_team, healthviro.example, 8; credentialing, healthviro.example, 8; dental_imaging, healthviro.example, 8; document_general_inbox, healthviro.example, 9; access_feedback, healthviro.example, 8; outpatient_admin_inbox, healthviro.example, 9; regional_outreach_inbox, healthviro.example, 9; outpatient_services_inbox, healthviro.example, 9; community_programs_inbox, healthviro.example, 9; regional_clinic_inbox, healthviro.example, 9; employeebenefits, healthviro.example, 8; enrollment_ops, healthviro.example, 8; medicalrecords_report2, healthviro.example, 8; familymedicine_schedules, healthviro.example, 9; helpdesk_inbox, healthviro.example, 9; clinic_generalbox, healthviro.example, 8; hr_inbox, healthviro.example, 9; internal_news, healthviro.example, 16; clinical_triage_1, healthviro.example, 8; dental_scan_queue, healthviro.example, 9; clinic_inbox, healthviro.example, 8; scanner_ops, corp.healthviro.example, 8; Healthviroconnect, healthviro.example, 8; Healthviromembercommun, healthviro.example, 8; Healthviroroc, healthviro.example, 12; hvcbehavioralhealth, healthviro.example, 15; mailflow, healthviro.example, 8; mycharthelp, healthviro.example, 8; obgynurgentline, healthviro.example, 17; payroll_inbox, healthviro.example, 9; pharmacyeligibility, healthviro.example, 8; pharmacypurchasing, healthviro.example, 12; preventioniscare, healthviro.example, 8; restrictedencounter, healthviro.example, 8; schoolhealth, healthviro.example, 8; ssiforms, healthviro.example, 8; urgentcare_inbox, healthviro.example, 9; streetmedreferrals, healthviro.example, 8; tobaccotreatment, healthviro.example, 8; compliance_inbox, healthviro.example, 9; eligibility_inbox, healthviro.example, 9; wellnesscenter, healthviro.example, 8; media_training, corp.healthviro.example, 10; conference_ops, healthviro.example, 10

High-data-access users:
None added to this finding beyond the privileged operational accounts above.

Regular users:
None. This finding is intentionally limited to higher-impact accounts.

Organization Notes
This is the priority reset list if the organization wants a smaller first wave. It is small enough to action quickly and important enough to matter immediately. It covers the accounts most likely to help an attacker move, persist, or cause disruption without needing Domain Admin access.

Remediation
Description
Reset and redesign high-impact non-human and privileged operational accounts first.

Minimum role required
Senior Active Directory or identity engineer; platform owners or service owners for workflow accounts.

Up to 3 remediation options

1. Preferred: Immediate reset and ownership review of all cracked high-impact accounts.
2. Reset the privileged operational accounts first, then the service/shared-function accounts in waves.
3. Disable unused shared-function accounts first, then reset the rest.

Preferred option and why
Option 1 is preferred because it cuts the most dangerous exposure first.

Remediation steps

1. Confirm business owner and purpose for every cracked high-impact account.
2. Immediately reset all privileged operational accounts.
3. Reset all named service, shared inbox accounts, mailbox-style, and shared-function accounts.
4. Move eligible accounts to managed secrets or supported service-account models.
5. Remove or disable accounts with no clear owner or no current business need.
6. Retest dependent systems after the reset.

Quick self-check

- All 160 high-impact accounts have been reset, disabled, or redesigned
- Each remaining account has a real owner
- Dependent systems still function after changes

Remediation references

- MITRE ATT&CK: T1078, T1078.002, T1078.001
- NIST SP 800-63B

Remediation Note
For this sample environment, this is the cleanest first remediation package because it is small, high-value, and easy to explain. If time is limited, do this list before the broader general-user cleanup.

Effort Estimate
High (>1 Day)

Evidence

- 160 high-impact enabled accounts were in the cracked population
- 153 were service, domain, shared-function, or similar operational accounts
- 8 were adminCount=1 privileged operational accounts
- 0 Domain Admin accounts were cracked

Known References

- MITRE ATT&CK: T1078 Valid Accounts; T1078.002 Domain Accounts; T1078.001 Default Accounts
- NIST SP 800-63B password guidance

3. Category: Weak Credentials — Passwords Below the Effective Policy Length and Common Construction Patterns

Security Risk Score: 8.9/10

Risk
If many passwords are shorter than the effective policy baseline or built from common patterns, attackers can crack them far more easily. That raises the chance of account takeover, internal spread, and business disruption. It also shows weak real-world password quality.

Issue
Short passwords and simple construction patterns reduce the work needed for successful cracking.

- Common words, branded terms, and simple letter-number combinations are easier to solve
- Reuse makes a cracked password more dangerous
- Weak construction broadens the set of accounts an attacker can exploit

Susceptibility
This is most exploitable when attackers obtain password hashes or other credential material and apply standard attacker password cracking techniques. Short length, common structure, and branded patterns make success more likely across large active populations.

Organization Notes
This sample environment had 1,163 enabled cracked accounts (79.4%) with passwords shorter than the current 14-character baseline. In the same cracked population, 1,005 accounts (68.6%) used letters and numbers only with no special characters, and 1,170 accounts (79.9%) used passwords containing HVC or Healthviro.

These populations overlap heavily. Taken together, the data shows that a large share of the active credential set was built from short, simple, or organization-branded patterns that standard attacker password cracking techniques can solve efficiently. This finding is separate from password reuse. Reuse makes one cracked password more dangerous. This finding explains why so many passwords were cracked in the first place.

Scoring

- Final Adjusted Score: 8.9
- CVSS 4.0 Environmental Score: 8.0
- BTE Adjustment: +0.9

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- Very large share of cracked accounts fell below the current 14-character standard
- Common branded and simple construction patterns materially increased cracking success
- Exposure was broad across active user and operational populations
- The finding explains the cracking outcome, not just the cracking count

Targets
Target count: 1,163 enabled accounts

Highly privileged:
privileged_ops_002, healthviro.example, 8; privileged_ops_003, healthviro.example, 10

Service/domain/operational accounts:
Large numbers of affected accounts existed in exam, kiosk, shared inbox, and shared-function populations, including clinical_credentialing_inbox, healthviro.example, 9; clinical_shared_inbox, healthviro.example, 9; accounts_payable, healthviro.example, 6; wellness_ops, healthviro.example, 8; billing, healthviro.example, 8; carecoordination_team, healthviro.example, 8; dental_imaging, healthviro.example, 8; access_feedback, healthviro.example, 8; scanner_ops, corp.healthviro.example, 8; Healthviroconnect, healthviro.example, 8; Healthviromembercommun, healthviro.example, 8; mailflow, healthviro.example, 8; mycharthelp, healthviro.example, 8; schoolhealth, healthviro.example, 8; ssiforms, healthviro.example, 8; streetmedreferrals, healthviro.example, 8

High-data-access users:
user_data_019, healthviro.example, 12; user_data_020, healthviro.example, 9; user_data_021, healthviro.example, 13; user_data_022, healthviro.example, 12; user_data_018, healthviro.example, 11

Regular users:
Large affected groups existed across ClinicExam01-ClinicExam10, AccessCheck01-AccessCheck08, ProviderExam01-ProviderExam10, OpsExam01-OpsExam17, training01-training12, DentalOps01-DentalOps14, intakecheck01-intakecheck04, wellnesscheck01-wellnesscheck02, wardA_exam01-wardA_exam10, wardB_exam01-wardB_exam09, wardC_exam01-wardC_exam09, plus many standard user accounts below the current length baseline.

Organization Notes:
This is the construction-quality finding. It explains why cracking success was so broad. The active password set was not only reused; it was also short, simple, and heavily branded. That means the organization should not treat this as a one-time cleanup. It is also a password-creation and account-governance problem.

Remediation:
Description
Reset passwords that fall below the effective standard and stop use of common branded or simple construction patterns.

Minimum role required
Active Directory engineer; help desk analyst for user coordination; security analyst for pattern review.

Up to 3 remediation options

1. Preferred: Force reset affected accounts and reject common branded or predictable patterns during reset.
2. Reset affected accounts in waves, starting with operational and high-access populations.
3. Apply stronger controls only to targeted high-risk groups first, then expand.

Preferred option and why
Option 1 is preferred because it directly removes the current weak-password population.

Remediation steps

1. Identify all cracked accounts whose passwords were shorter than the effective standard or showed common construction patterns.

2. Force reset those accounts.
3. During reset, instruct users and operators to avoid branded, sequential, or simple letter-number patterns.
4. Review shared-function and template workflows that keep recreating the same patterns.
5. Add blocklist or screening logic where practical for obvious common patterns.
6. Recheck the affected population after remediation.

Quick self-check

- Affected accounts no longer use substandard lengths or obvious common patterns
- The cracked population with short/simple passwords drops materially after reset
- New passwords no longer cluster around branded naming patterns

Remediation references

- NIST SP 800-63B

Remediation Note

For this sample environment, use this finding to drive user-facing reset instructions. Make it explicit that the problem is not just “bad-looking” passwords. Many cracked passwords were simply too short, too common, or too familiar in structure.

Effort Estimate

Medium (<1 Day)

Evidence

- 1,163 / 1,465 cracked enabled accounts were shorter than 14 characters
- 1,005 / 1,465 cracked enabled accounts used letters and numbers only
- 1,170 / 1,465 cracked enabled accounts contained HVC or Healthviro
- 665 / 1,465 cracked enabled accounts were exactly 8 characters

Known References

- MITRE ATT&CK: T1110.002 Password Cracking
- NIST SP 800-63B password guidance, including minimum lengths and blocklist checks

4. Category: Operational Policy — Non-Expiring Passwords on Enabled Accounts

Security Risk Score: 8.7/10

Risk
Passwords that never expire stay valid until someone changes them by hand. If those passwords are weak or already cracked, an attacker can keep using them for much longer than intended. That increases persistence risk.

Issue
Non-expiring passwords sit outside the normal password-change cycle.

- That is especially dangerous for service, shared, kiosk, or other long-lived operational identities
- If those same accounts also use weak or shared passwords, the problem gets much worse
- Cleanup is harder because stale exceptions stay live longer

Susceptibility
This is easy to exploit because a cracked password can stay useful indefinitely if nobody resets it. Attackers get the most value when non-expiring passwords belong to service or operational accounts that touch many systems.

Organization Notes
There were 1,358 enabled Active Directory user accounts with passwords set to never expire. Of the 1,465 enabled user accounts whose passwords were cracked, 953 accounts, or 65.1%, were also non-expiring. This overlap is what makes the issue serious. Many of the passwords cracked during the assessment could stay valid indefinitely unless they are deliberately reset. The problem was concentrated in service accounts, kiosk and exam accounts, shared operational identities, and other long-lived accounts used in daily workflows.

Scoring

- Final Adjusted Score: 8.7
- CVSS 4.0 Environmental Score: 7.9
- BTE Adjustment: +0.8

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- Large non-expiring population overlapped directly with cracked accounts
- Non-expiring credentials increase persistence value for an attacker. The issue was concentrated in operational and service-style accounts.
- Cleanup failures would leave long-lived access paths in place

Targets
1,358 enabled non-expiring accounts; 953 of those were already compromised.

Highly privileged:
Privileged non-expiring service or domain accounts included svc_reporting_001, Svc_identitysync_001, Svc_cloudsync_001, svc_platform_001, svc_database_001, Svc_directory_001, svc_directory_002.

Compromised adminCount=1 operational accounts: Privileged_ops_001, privileged_ops_002, privileged_ops_003.

Service/domain/operational accounts:
Non-expiring and compromised service/domain accounts included accounts_payable, billing, scanner_ops, Healthviroconnect, Healthviromembercommun, mailflow, mycharthelp, pharmacyeligibility, schoolhealth, streetmedreferrals, conference_ops, and many of the shared inbox and shared-function identities listed in Findings 1 and 2.

High-data-access users:
A smaller set of named higher-impact users also appeared in the cracked non-expiring population, though the main concentration was in service and operational accounts.

Regular users:
Large non-expiring populations existed in kiosk and exam account sets, dental operational accounts, shared inbox identities, shared mailboxes, legacy utility accounts, and template-derived operational accounts.

Organization Notes
The core problem is the overlap. A large number of accounts were both non-expiring and cracked. That means many of the credentials exposed during the assessment can remain usable until the organization actively changes them. This is one of the biggest reasons weak and reused passwords stayed live in the environment.

Remediation
Description
Cut down the non-expiring population to the smallest defensible set and replace static operational passwords with managed alternatives.

Minimum role required
Senior Active Directory or identity engineer; platform owners for service-account dependencies.

Up to 3 remediation options

1. Preferred: Remove non-expiring settings from all human accounts and move eligible service accounts to managed credential models.
2. Keep a small approved exception list but require strong unique passwords and named ownership.
3. Keep the current model temporarily but force immediate reset and quarterly review of all non-expiring accounts.

Preferred option and why
Option 1 is preferred because it removes the persistence problem instead of just documenting it.

Remediation steps

1. Export every enabled non-expiring account and assign a real owner.
2. Remove the non-expiring setting from all user accounts unless there is a documented business reason.
3. Reset all cracked non-expiring accounts immediately.
4. Replace static service-account passwords with managed secrets or supported service-account technologies.

5. Disable non-essential legacy or convenience accounts.
6. Review the remaining exception list on a fixed schedule.

Quick self-check

- The non-expiring population is reduced to a small approved service-only list
- All cracked non-expiring accounts have been reset
- Each remaining exception has an owner and written business justification

Remediation references

- NIST SP 800-63B

Remediation Note

For this sample environment, the biggest short-term win is to reset all cracked non-expiring accounts first, then remove non-expiring settings from named user accounts and template-derived identities.

Effort Estimate

High (>1 Day)

Evidence

- 1,358 enabled user accounts set to password never expires
- 953 cracked enabled accounts also non-expiring
- All 8 compromised adminCount=1 accounts were also non-expiring
- Privileged non-expiring service/domain accounts existed even where not cracked

Known References

- MITRE ATT&CK: T1078 Valid Accounts; T1078.002 Domain Accounts
- NIST SP 800-63B password guidance

5. Category: System Policy — Password Policy Gaps and Exception Drift

Security Risk Score: 8.0/10

Risk
A password policy can look decent on paper and still fail in practice. If the rules are weak, easy to work around, or not applied consistently, attackers still get plenty of weak passwords to target. That creates hidden risk.

Issue
A zero minimum password age and a short password history make it easier for people to cycle back to familiar passwords.

- A stronger fine-grained policy only helps if it is actually applied
- Heavy use of non-expiring accounts weakens the effective control
- Policy intent and live outcomes are not aligned

Susceptibility
Attackers do not need every setting to be weak. They only need enough legacy passwords, policy exceptions, or weak operational practices to keep exploitable passwords alive. A written baseline may stop some basic guessing while still leaving real exposure.

Organization Notes
The default password policy was better than many environments, but it was not strong enough in practice to prevent the results seen here. The default domain policy was minimum length 14, complexity enabled, password history 5, minimum password age 0, maximum password age 365 days, and lockout after 3 attempts for 15 minutes. A fine-grained policy existed with minimum length 16, but the active results show it did not correct the weak-password population in scope. The most important gaps were the minimum password age of zero, history of only five, and the heavy operational use of non-expiring accounts.

Scoring

- Final Adjusted Score: 8.0
- CVSS 4.0 Environmental Score: 7.4
- BTE Adjustment: +0.6

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- The written baseline looked better than the real outcomes
- Policy settings and exceptions allowed weak passwords to remain active
- The effective control was materially weaker than the configured intent
- Strong practical results were not visible in the enabled cracked population

Targets
Target count: Domain-wide policy plus all enabled user accounts in scope

Policy settings:
Domain, corp.healthviro.example, minimum password length 14; password history count 5; complexity enabled True; reversible encryption enabled False; minimum password age 00:00:00; maximum password age 365.00:00:00; lockout threshold 3; lockout duration 00:15:00; lockout observation window 00:15:00

Fine-grained policies:
Default HVC Password Policy, precedence 1, minimum length 16; maximum age 365.00:00:00; lockout threshold 3; complexity True

Organization Notes
The baseline policy is not the worst part of the environment. The problem is that the active passwords did not reflect that baseline. The environment still had a large number of cracked passwords, extensive password reuse, heavy use of branded password patterns, and many non-expiring accounts. In plain terms, the policy may exist, but the outcome is still weak.

Remediation
Description
Tighten the effective password policy and close the gaps created by exceptions.

Minimum role required
Senior Active Directory or identity engineer; IT leadership for policy approval and rollout.

Up to 3 remediation options

1. Preferred: Tighten the baseline and reduce exceptions at the same time.
2. Keep the baseline mostly as-is but fix exception drift and force reset weak accounts.
3. Apply stronger fine-grained policy to targeted account sets first.

Preferred option and why
Option 1 is preferred because it fixes both policy and outcome.

Remediation steps

1. Set a non-zero minimum password age.
2. Increase password history beyond five.
3. Verify that the fine-grained policy is actually applied to the intended account groups.
4. Remove password-expiry exceptions unless there is a documented business reason.
5. Force reset accounts that still fall below the intended standard.
6. Review templates, kiosk accounts, service identities, and shared operational accounts on a regular schedule.

Quick self-check

- Minimum password age is no longer zero
- Password history is deeper than five
- Fine-grained policy assignment is real and verifiable
- Weak-password populations drop after reset and enforcement

Remediation references

- NIST SP 800-63B

Remediation Note

For this sample environment, policy changes should not be done alone. They need to be tied directly to a reset campaign or the current weak-password population will remain active.

Effort Estimate

Medium (<1 Day)

Evidence

- Default domain minimum length: 14
- Fine-grained minimum length: 16
- Password history count: 5
- Minimum password age: 0
- Maximum password age: 365 days
- Lockout threshold: 3
- Enabled non-expiring accounts: 1,358
- Cracked enabled accounts: 1,465

Known References

- NIST SP 800-63B password guidance
- MITRE ATT&CK context: T1110 Password-related brute force techniques; T1078 Valid Accounts

6. Category: Weak Credentials— Residual Compromised Password Exposure

Security Risk Score: 7.6/10

Risk
Some passwords may still be cracked even when they do not fall into the obvious buckets like reuse, short length, or non-expiring status. If an attacker can crack them, they still have to be treated as compromised. That still creates real access risk.

Issue
These are enabled accounts whose passwords were cracked but were not directly captured as targets in the earlier more-specific findings.

- That does not mean the passwords were strong
- It means they were still solvable with attacker techniques
- From an attacker's point of view, cracked means compromised

Susceptibility
This is exploitable anywhere an attacker can obtain password hashes or other credential material and apply standard attacker password cracking techniques. Even if a password does not look obviously weak, successful cracking proves it can be solved.

Organization Notes
This is the required residual finding. It captures the remaining enabled cracked accounts that were not already directly represented as target accounts in the earlier more-specific findings for password reuse, privileged/service exposure, non-expiring passwords, short/simple construction, or policy drift. In this sample environment, that residual set contains 163 enabled user accounts. These accounts matter because they prove the organization still had additional active credentials that attackers could crack even when those accounts did not fit the more obvious patterns. Some of these passwords are longer and do not look immediately weak to a human reviewer, but they were still cracked. From a practical risk standpoint, they should be treated the same way: compromised and in need of reset.

Scoring

- Final Adjusted Score: 7.6
- CVSS 4.0 Environmental Score: 7.0
- BTE Adjustment: +0.6

BTE is a Business-Threat-Exposure overlay that adjusts the environmental score to reflect real business impact, proven attacker practicality, and the actual spread of exposure shown in the assessment.

Justification

- Proven exploitability: these passwords were still cracked
- Residual exposure remained after the more specific higher-risk groups were separated out
- The score was anchored to the highest-value accounts present in this residual set
- The presence of longer cracked passwords shows the residual set cannot be ignored

Targets
Target count: 163 enabled accounts

Highly privileged:
user_data_001, healthviro.example, 14; user_data_002, healthviro.example, 17; user_data_003, healthviro.example, 14; user_data_013, healthviro.example, 14

Service/domain/operational accounts:
None in this residual set.

High-data-access users:
user_data_017, healthviro.example, 15; user_data_005, healthviro.example, 15; user_data_023, healthviro.example, 14; user_data_024, healthviro.example, 15; user_data_025, healthviro.example, 14; user_data_015, healthviro.example, 14; user_data_026, healthviro.example, 14; user_data_027, healthviro.example, 14; user_data_028, healthviro.example, 14

Regular users:
mhayes, healthviro.example, 15; aokafor, healthviro.example, 17; jmarin, healthviro.example, 14; pnovak, healthviro.example, 14; nfarouk, healthviro.example, 14; tnguyen, healthviro.example, 14; rbellamy, healthviro.example, 19; ksingh, healthviro.example, 14; cdelaney, healthviro.example, 17; morozco, healthviro.example, 15; ewhitaker, healthviro.example, 14; lpetrov, healthviro.example, 15; savramov, healthviro.example, 14; ebarrow, healthviro.example, 15; fgriffin, healthviro.example, 14; gsilva, healthviro.example, 14; hsexton, healthviro.example, 16; jkarim, healthviro.example, 16; jmelton, healthviro.example, 15; jstokes, healthviro.example, 14; koda, healthviro.example, 15; kjackson, healthviro.example, 15; lharper, healthviro.example, 17; lcamden, healthviro.example, 16; marias, healthviro.example, 15; mprice, healthviro.example, 14; mbennett, healthviro.example, 14; eghani, healthviro.example, 14; mchavarria, healthviro.example, 14; sdraper, healthviro.example, 14; nroth, healthviro.example, 21; pgallagher, healthviro.example, 15; rhicks, healthviro.example, 15; rlane, healthviro.example, 14; sbeier, healthviro.example, 14; scortez, healthviro.example, 14; sshannon, healthviro.example, 15; sjansen, healthviro.example, 17; sramirez, healthviro.example, 14; swolfe, healthviro.example, 14; ysato, healthviro.example, 16

Organization Notes
This is the remaining cracked-password population after the more specific categories were broken out. These accounts should not be ignored simply because they were not part of the bigger headline groups. They still represent confirmed password compromise and need to be reset.

Remediation
Description
Reset the remaining cracked passwords, confirm they meet current policy, and increase uniqueness and complexity where appropriate.

Minimum role required
Active Directory engineer; help desk analyst.

Up to 3 remediation options

1. Preferred: Force reset all residual cracked accounts.
2. Reset these accounts in small business-unit waves.
3. Pair reset with user guidance on stronger unique password creation.

Preferred option and why
Option 1 is preferred because these passwords are already proven compromised.

Remediation steps

1. Export the residual cracked-account list.
2. Force reset these passwords.
3. Make sure new passwords meet current policy and avoid familiar or reused patterns.
4. Provide simple user guidance on choosing stronger unique passwords.
5. Recheck this residual set after resets complete.

Quick self-check

- All residual cracked accounts have been reset
- New passwords meet policy
- None of these accounts remain in the cracked population after recheck

Remediation references

- NIST SP 800-63B

Remediation Note

Pre: After the organization completes the higher-priority grouped findings, use this residual list as the final cleanup queue so no known cracked enabled account is left unresolved.

Effort Estimate

Medium (<1 Day)

Evidence

- 163 enabled cracked accounts remained after the more specific direct-target findings were separated out
- Residual set included passwords from 14 to 21 characters
- Residual set had 0 non-expiring accounts and was outside the reused-password direct-target population by design

Known References

- MITRE ATT&CK: T1110.002 Password Cracking; T1078 Valid Accounts
- NIST SP 800-63B password guidance

Positive Findings – What They Are Doing Well

No Domain Admin passwords were cracked
The highest-value administrative tier held up. That prevented an already serious password problem from becoming a direct top-tier administrative failure.

No enabled user accounts had blank passwords
None of the enabled Active Directory user accounts in scope had a blank password. That removes one of the most basic and dangerous credential failures.

Password complexity is enabled at the domain level
Complexity is turned on in the default policy. That is a necessary baseline and better than environments still relying on very weak composition rules.

The baseline minimum password length is not trivial
The default policy minimum is 14 characters, and a fine-grained policy with 16 characters also exists. The control intent is better than many peer environments, even though the live results show it is being undermined.

Account lockout is configured
Lockout after 3 failed attempts with a 15-minute duration and observation window helps reduce basic online guessing and spraying.

Reversible password storage is disabled
Passwords are not stored with reversible encryption. That is the correct setting and avoids a serious credential-storage weakness.