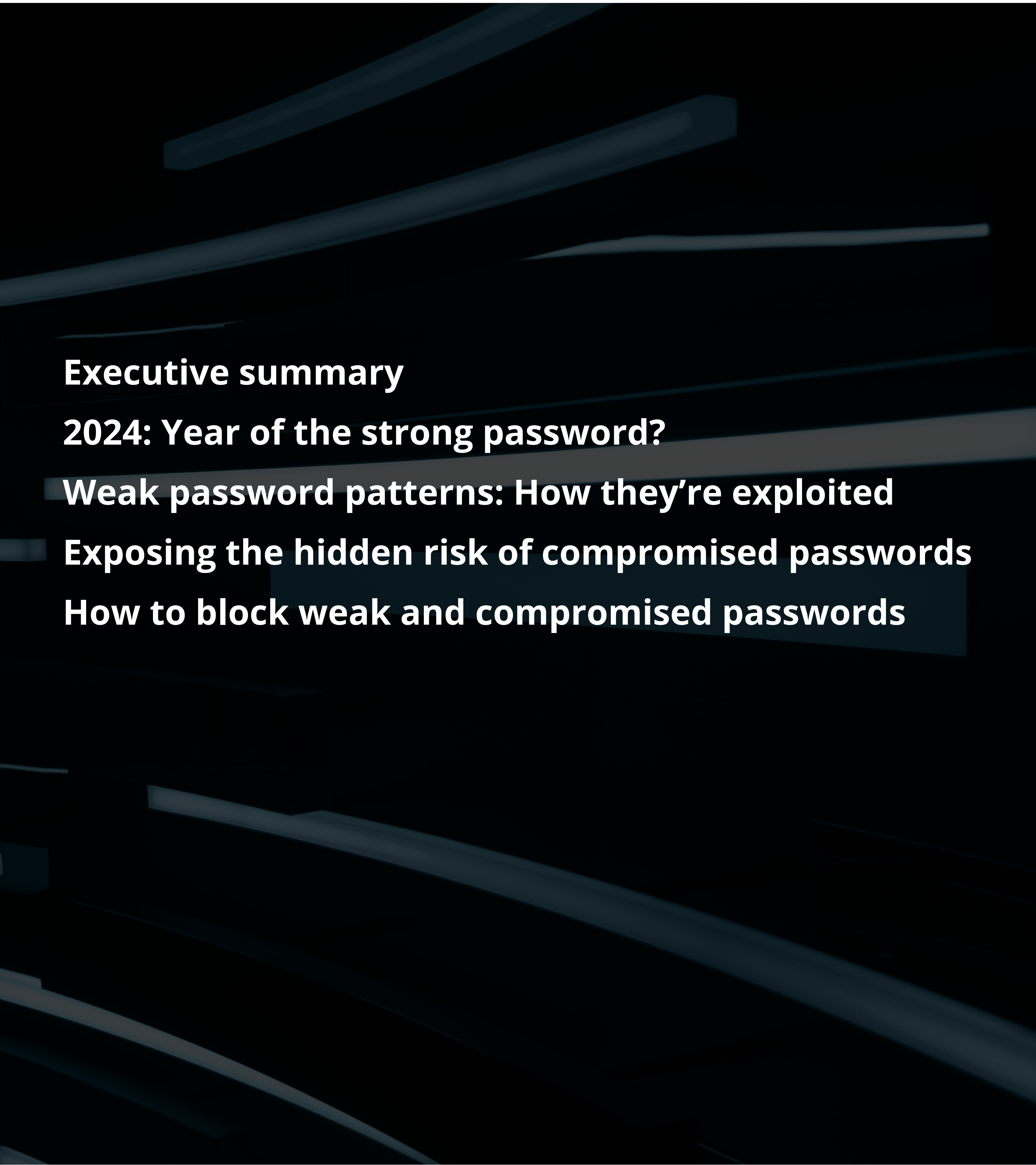
SPECOPS
AN OUTPOST24 COMPANY

# Breached Password Report

2024

Latest research into the trends and patterns of weak and compromised passwords.

## What's inside?



# Executive summary

## Report highlights

**Here are some of the key stats and findings we've picked out from the 2024 Breached Password Report:**

123456 was the most common compromised password found in KrakenLab's new list of breached cloud application credentials[1]

Simple passwords like Pass@123 and P@ssw0rd that would pass Active Directory's basic built-in rules were also found to be prevalent, highlighting the increased risk of password reuse for organization's not implementing strong password controls[1]

KrakenLab compromised application credential research suggests that a required Active Directory password length of at least 13 would greatly reduce the danger of cloud application password reuse in Active Directory environments[1]

After analyzing 1.8 million breached administrator credentials, 40,000 admin portal accounts were found to be using 'admin' as a password[2]

88% of organizations still use passwords as their primary method of authentication[3]

Only 50% of organizations scan for compromised passwords more than once a month[3]

Keyboard walks such as 'qwerty' are weak passwords used by millions of end users[4]

Longer passwords aren't safe from being breached – we found 31.1 million breached passwords to be over 16 characters in length[4]

Long passwords hashed with MD5 and bcrypt can take millions of years to crack – but password reuse can render them immediately compromised[4]

## Methodology

**Data in this report comes from the sources detailed below – some has been previously published throughout the year while some is brand new. We'll make it clear which pieces of information come from which source as you read through:**
The Outpost24 (Specops Software's parent company) threat intelligence team, KrakenLabs, carried out two pieces of research detailed in this report:

1. Analyzed more than two million business application credentials hacked by malware to find some of the most commonly breached passwords. Published for this first time in this report1

2. Analyzed 1.8 million administrator credentials collected between January and September 20232

3. Specops surveyed 151 cybersecurity professionals at the 2023 International Cyber Expo event. Participants were asked a set of in-person questions about their organization's password security – these responses are detailed in this report for the first time. All respondents and their respective organizations remained anonymous

4. Over the past year, Specops researchers have run several pieces of analysis on a pool of over 800 million breached passwords. This is a subset of our larger Breached Password Protection database of over 4 billion breached passwords

# Introduction

## 2024: Year of the secure password?

After decades of end user training, passwords are still a problem for IT teams and a weak point in many organization's cybersecurity strategies. A huge amount of cybercrime still focuses on passwords: stealing credentials, selling them on, and using them as an initial access point for breaching organizations. Verizon estimates stolen credentials are involved in nearly half (44.7%) of all data breaches, and we know there's a thriving underground marketplace for stolen data and credentials.

Despite this, passwords aren't going anywhere. We surveyed 151 cybersecurity professionals at the 2023 International Cyber Expo event and found that only 12% of organizations have moved away from using passwords as their primary method of authentication. Getting rid of passwords entirely is simply not feasible for most organizations – so how can we make them work better?

Throughout 2023, our research team regularly analyzed breached password data and live attacks to share their findings and showcase the importance of password security and potential vulnerabilities posed by weak or compromised passwords. This report brings the highlights of that research together along with some previously unpublished findings. The aim is to give organizations a deeper understanding of the patterns and trends relating to breached passwords, as well as sharing advice on how to tighten up their access security.

We'll explore how weak and compromised passwords offer potential attack routes into organizations, why a strong password policy isn't enough on its own and explore some of the password mistakes you might not know your end users are making. You'll also get access to a free Active Directory auditing tool and practical advice from our years of password security expertise that can be implemented straight away.

Make 2024 the year of the secure password!

*– Darren James, Senior Product Manager*

# Weak password patterns: How they're exploited

It would be hard to find an end user who hasn't been given at least some training on what makes a weak password. However, years of best practice recommendations haven't hammered home the importance for the average employee. Our 2023 Weak Password Report found that the most common base terms used in breached passwords were "password", "admin", and "welcome" – terms you'd think would be obviously off-limits to any security-savvy end user. Weak passwords remain the gifts that keep on giving for hackers seeking an easy entry route into organizations.

But how exactly do hackers exploit weak passwords like "Winter2024"? And what weak passwords are end users making that might be slipping through your password policies? We'll explore both problems and also look at some admin password data to see how well protected the most privileged accounts are.

## Three ways hackers exploit weak passwords

### Dictionary attack

Hackers use predefined 'dictionary lists' of likely possibilities to guess passwords or decryption keys. These could range from frequently used passwords and common phrases to common terms in specific industries, exploiting the human tendency to opt for simplicity and familiarity when creating passwords.

Hackers use social media platforms to gather intel about specific users and their organizations, gaining insights into the potential usernames and passwords they may choose. Of course, many end users will add at least a small amount of variation to these terms, which is where brute force techniques come in.

### Brute force attack

Brute force attacks use software to attempt all possible character combinations until the correct password or decryption key is found. While this might seem time-consuming, it can be highly effective against shorter or less complex passwords – especially when given a head start by using common base terms found in dictionary lists. Combining techniques in this way is known as a hybrid attack.

For example, "password" could be the base term from a dictionary list. A brute force attack will try all subsequent variations such as "password, Password, Password1, Password!" and so on. This takes advantages of the common variations people make to weak base terms in order to meet their organization's complexity requirements.

### Mask attack

A mask attack is a form of brute forcing, where attackers know elements of common password constructions and can therefore reduce the amount of guesses they'll need to get it right. For example, an attacker might know many passwords are eight characters, start with a capital letter, and end with a number of punctuation character, like "Welcome1!". So they might only try combinations that match this pattern, reducing the total amount of passwords to attempt.

Alternatively, they might know a specific company has a poor policy such as adding the current month and year to the end of passwords when rotating them. Having any sort of definitive information about the makeup of a password can greatly speed up a brute force attack.

## Keyboard walks

At first glance, “asdfghjkl” might seem like a random base term for a password. However, this is known as a keyboard walk, where characters are next to each other on a keyboard. People choose these ‘finger walks’ as passwords as they’re fast to type and easy to remember when looking at a keyboard.

While the output isn’t a real word, hackers know to include these common patterns in their dictionary and brute force attacks. As highlighted previously in the hacker’s tactics, end user predictability is a key aspect of password hacking.

### Top Qwerty Keyboard Walk Patterns Found in Compromised Passwords

In 2023, the Specops research team dedicated some specific research to the use of keyboard walk patterns, analyzing over 800 million passwords (a subset of our Breached Password Protection database of over 4 billion breached passwords). They discovered some alarming trends. The most commonly used keyboard walk pattern was “Qwerty,” which appeared over 1 million times in our list of compromised passwords.

This was followed by variations like “qwert” and “werty” as well as patterns specific to different keyboard layouts such as “Azerty”. It serves as a reminder to organizations that it’s key to block all kinds of predictable password behavior – not just common words.

## Do admins know better?

Skilled hackers can elevate privileges from a regular user account, so all accounts are worth protecting. Still, existing admin accounts already hold the so-called "keys to the kingdom" due to the level of access they hold without any need for privilege escalation. Compromising an admin account is a dream scenario for a hacker, as they'll have more options after gaining initial access to an organization. So surely these accounts have stronger passwords than those held by the average end user?

Concerningly, a recent study by our parent company Outpost24 revealed over 40,000 admin portal accounts are using the weak password "admin" to protect access to some of the most sensitive accounts with the highest levels of access within an organization. Researchers analyzed more than 1.8 million administrator credentials collected between January and September 2023, highlighting the risk of weak passwords being easily guessed by hackers.

Privileged users are golden targets for hackers. Strong, unique passwords are needed for every account, but especially those with access to sensitive resources. As you can see from the table below, this wasn't the case in real breached password data our team analyzed. Note the prevalence of keyboard walks too.

| Most commonly breached (descending order) | Breached admin passwords |
|---|---|
| 1 | admin |
| 2 | 123456 |
| 3 | 12345678 |
| 4 | 1234 |
| 5 | Password |
| 6 | 123 |
| 7 | 12345 |
| 8 | Admin123 |
| 9 | 123456789 |
| 10 | adminisp |
| 11 | demo |
| 12 | root |
| 13 | 123123 |
| 14 | admin@123 |
| 15 | 123456aA@ |
| 16 | 01031974 |
| 17 | Admin@123 |
| 18 | 111111 |
| 19 | admin1234 |
| 20 | admin1 |

## Specops analysis: What makes a strong password?

If your policy extends the required length of passwords beyond the standard Active Directory limit of eight characters, you'll be making it significantly more difficult for brute force attacks to succeed. This is true even if hackers have access to substantial computing power.

We strongly recommend forcing end users to create passwords that are at least 15 characters long – ideally over 20 characters. A great method to make this work is to encourage passphrases consisting of three random words, which are far easier for end users to remember. For instance, "Hazily-Garden-Baboon" is more memorable than a string of eight random numbers and also more secure. Adding in a couple of special characters or deliberately misspelling a word would make this example a very strong passphrase.

Specops solutions make sure to provide users with dynamic feedback as they create their passwords, allowing them to see which requirements they're meeting in real time. Organizations also have the option to implement length-based aging, where end users who create strong passwords are 'rewarded' with a longer period before their next password reset.

And of course, a critical point to remember is making sure a password has not been previously compromised. As if that's the case, the above methods count for nothing.

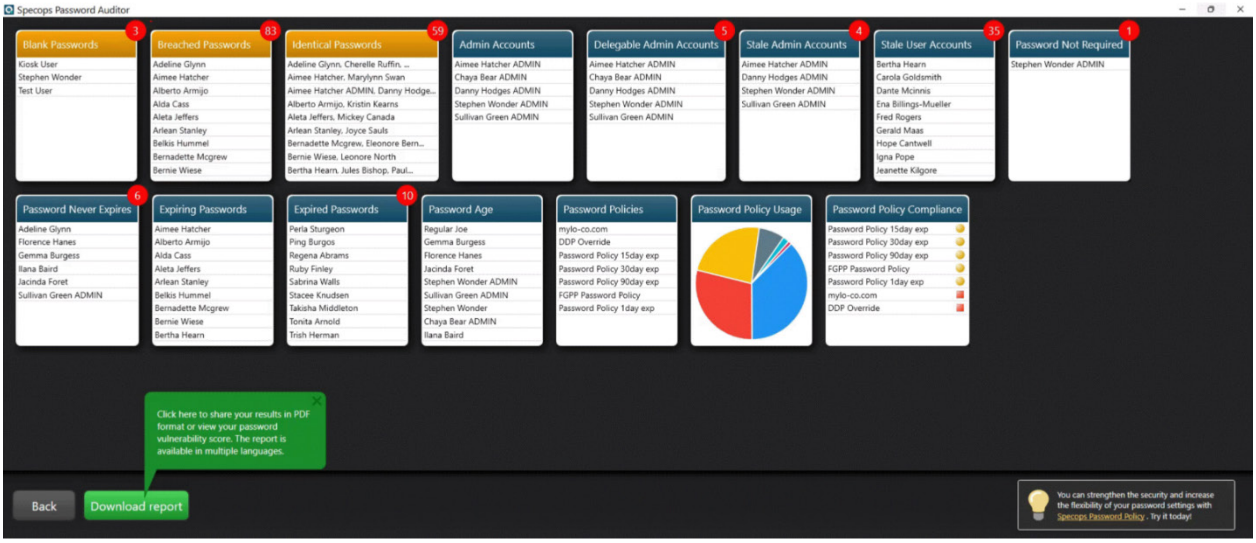
*– Darren James, Senior Product Manager*

# Are weak passwords hiding in your Active Directory? Run an audit today

An audit starts your journey towards better password security. Specops Password Auditor is a free tool that can identify multiple types of password-related vulnerability in minutes. Carry out a read-only check of your Active Directory against almost 1 billion compromised passwords and analyze your domain password policies and fine-grained password policies. You can also learn whether your policies are compliant with common cybersecurity regulations.

**Your exportable report will give you visibility over the following information and password-related vulnerabilities:**

- Breached passwords
- Blank passwords
- Identical passwords
- Stale admin accounts
- ‘Password not required’ accounts
- Stale user accounts
- ‘Password never expires’ accounts
- Expired passwords
- Password policies + usage
- Password policy compliance



Blank Passwords 3
- Kiosk User
- Stephen Wonder
- Test User

Breached Passwords 83
- Adeline Glynn
- Aimee Hatcher
- Alberto Armijo
- Alda Cass
- Aleta Jeffers
- Arlean Stanley
- Belkis Hummel
- Bernadette Mcgrew
- Bernie Wiese

Identical Passwords 59
- Adeline Glynn, Cherelle Ruffin, ...
- Aimee Hatcher, Marylynn Swan
- Aimee Hatcher ADMIN, Danny Hodge...
- Alberto Armijo, Kristin Kearns
- Aleta Jeffers, Mickey Canada
- Arlean Stanley, Joyce Sauls
- Bernadette Mcgrew, Eleonore Bern...
- Bernie Wiese, Leonore North
- Bertha Hearn, Jules Bishop, Paul...

Admin Accounts
- Aimee Hatcher ADMIN
- Chaya Bear ADMIN
- Danny Hodges ADMIN
- Stephen Wonder ADMIN
- Sullivan Green ADMIN

Delegable Admin Accounts 5
- Aimee Hatcher ADMIN
- Chaya Bear ADMIN
- Danny Hodges ADMIN
- Stephen Wonder ADMIN
- Sullivan Green ADMIN

Stale Admin Accounts 4
- Aimee Hatcher ADMIN
- Danny Hodges ADMIN
- Stephen Wonder ADMIN
- Sullivan Green ADMIN

Stale User Accounts 35
- Bertha Hearn
- Carola Goldsmith
- Dante Mcinnis
- Ena Billings-Mueller
- Fred Rogers
- Gerald Maas
- Hope Cantwell
- Igna Pope
- Jeanette Kilgore

Password Not Required 1
- Stephen Wonder ADMIN

Password Never Expires 6
- Adeline Glynn
- Florence Hanes
- Gemma Burgess
- Ilana Baird
- Jacinda Foret
- Sullivan Green ADMIN

Expiring Passwords
- Aimee Hatcher
- Alberto Armijo
- Alda Cass
- Aleta Jeffers
- Arlean Stanley
- Belkis Hummel
- Bernadette Mcgrew
- Bernie Wiese
- Bertha Hearn

Expired Passwords 10
- Perla Sturgeon
- Ping Burgos
- Regena Abrams
- Ruby Finley
- Sabrina Walls
- Stacee Knudsen
- Takisha Middleton
- Tonita Arnold
- Trish Herman

Password Age
- Regular Joe
- Gemma Burgess
- Florence Hanes
- Jacinda Foret
- Stephen Wonder ADMIN
- Sullivan Green ADMIN
- Stephen Wonder
- Chaya Bear ADMIN
- Ilana Baird

Password Policies
- mylo-co.com
- DDP Override
- Password Policy 15day exp
- Password Policy 30day exp
- Password Policy 90day exp
- FGPP Password Policy
- Password Policy 1day exp

Password Policy Usage

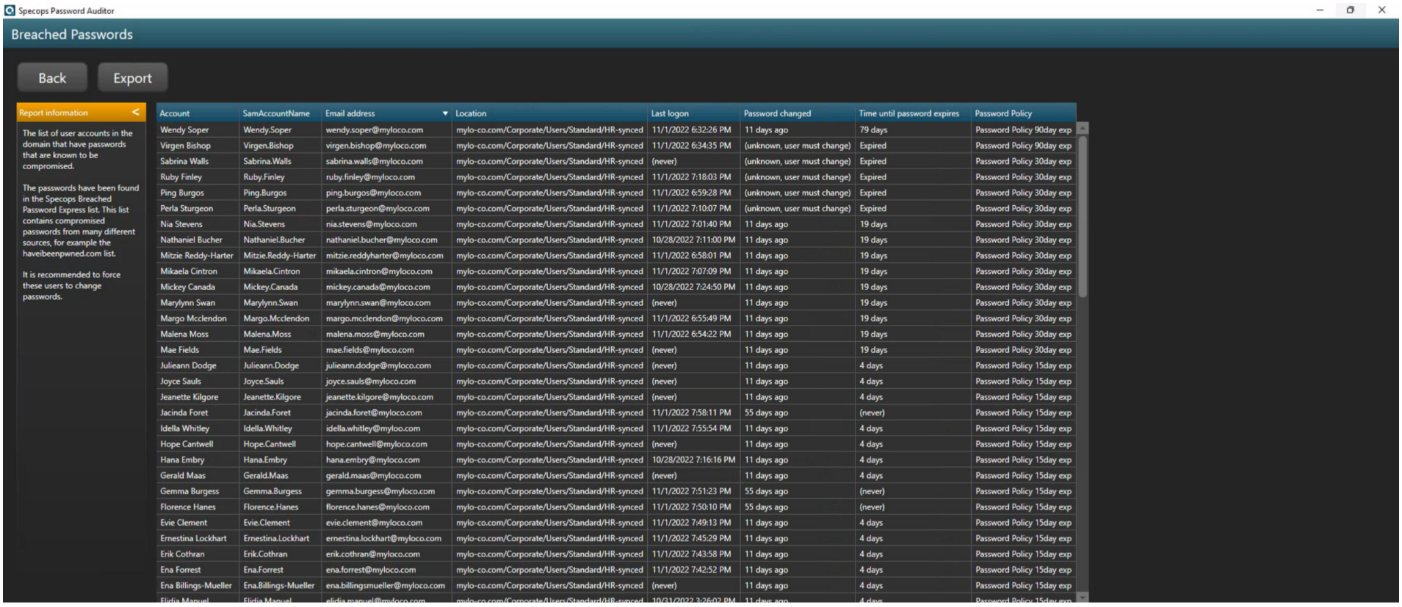
Password Policy Compliance
- Password Policy 15day exp ●
- Password Policy 30day exp ●
- Password Policy 90day exp ●
- FGPP Password Policy ●
- Password Policy 1day exp ●
- mylo-co.com 🟥
- DDP Override 🟥

Click here to share your results in PDF format or view your password vulnerability score. The report is available in multiple languages.

You can strengthen the security and increase the flexibility of your password settings with Specops Password Policy . Try it today!

*Specops Password Auditor: Results dashboard*

Remember to pay particular attention to end users with known breached or compromised passwords, as these offer a simple route into your organization for hackers:



The list of user accounts in the domain that have passwords that are known to be compromised.

The passwords have been found in the Specops Breached Password Express list. This list contains compromised passwords from many different sources, for example the haveibeenpwned.com list.

It is recommended to force these users to change passwords.

| Account | SamAccountName | Email address | Location | Last logon | Password changed | Time until password expires | Password Policy |
|---|---|---|---|---|---|---|---|
| Wendy Soper | Wendy.Soper | wendy.soper@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:32:26 PM | 11 days ago | 79 days | Password Policy 90day exp |
| Virgen Bishop | Virgen.Bishop | virgen.bishop@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:34:35 PM | (unknown, user must change) | Expired | Password Policy 90day exp |
| Sabrina Walls | Sabrina.Walls | sabrina.walls@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | (unknown, user must change) | Expired | Password Policy 30day exp |
| Ruby Finley | Ruby.Finley | ruby.finley@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:18:03 PM | (unknown, user must change) | Expired | Password Policy 30day exp |
| Ping Burgos | Ping.Burgos | ping.burgos@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:59:28 PM | (unknown, user must change) | Expired | Password Policy 30day exp |
| Perla Sturgeon | Perla.Sturgeon | perla.sturgeon@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:10:07 PM | (unknown, user must change) | Expired | Password Policy 30day exp |
| Nia Stevens | Nia.Stevens | nia.stevens@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:01:40 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Nathaniel Bucher | Nathaniel.Bucher | nathaniel.bucher@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 10/28/2022 7:11:00 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Mitzie Reddy-Harter | Mitzie.Reddy-Harter | mitzie.reddyharter@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:58:01 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Mikaela Cintron | Mikaela.Cintron | mikaela.cintron@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:07:09 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Mickey Canada | Mickey.Canada | mickey.canada@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 10/28/2022 7:24:50 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Marylynn Swan | Marylynn.Swan | marylynn.swan@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 19 days | Password Policy 30day exp |
| Margo Mcclendon | Margo.Mcclendon | margo.mcclendon@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:55:49 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Malena Moss | Malena.Moss | malena.moss@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 6:54:22 PM | 11 days ago | 19 days | Password Policy 30day exp |
| Mae Fields | Mae.Fields | mae.fields@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 19 days | Password Policy 30day exp |
| Julieann Dodge | Julieann.Dodge | julieann.dodge@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Joyce Sauls | Joyce.Sauls | joyce.sauls@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Jeanette Kilgore | Jeanette.Kilgore | jeanette.kilgore@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Jacinda Foret | Jacinda.Foret | jacinda.foret@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:58:11 PM | 55 days ago | (never) | Password Policy 15day exp |
| Idella Whitley | Idella.Whitley | idella.whitley@myloo.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:55:54 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Hope Cantwell | Hope.Cantwell | hope.cantwell@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Hana Embry | Hana.Embry | hana.embry@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 10/28/2022 7:16:16 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Gerald Maas | Gerald.Maas | gerald.maas@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Gemma Burgess | Gemma.Burgess | gemma.burgess@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:51:23 PM | 55 days ago | (never) | Password Policy 15day exp |
| Florence Hanes | Florence.Hanes | florence.hanes@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:50:10 PM | 55 days ago | (never) | Password Policy 15day exp |
| Evie Clement | Evie.Clement | evie.clement@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:49:13 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Ernestina Lockhart | Ernestina.Lockhart | ernestina.lockhart@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:45:29 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Erik Cothran | Erik.Cothran | erik.cothran@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:43:58 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Ena Forrest | Ena.Forrest | ena.forrest@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 11/1/2022 7:42:52 PM | 11 days ago | 4 days | Password Policy 15day exp |
| Ena Billings-Mueller | Ena.Billings-Mueller | ena.billingsmueller@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | (never) | 11 days ago | 4 days | Password Policy 15day exp |
| Elidia Manuel | Elidia.Manuel | elidia.manuel@myloco.com | mylo-co.com/Corporate/Users/Standard/HR-synced | 10/31/2022 3:26:02 PM | 11 days ago | 4 days | Password Policy 15day exp |

*Specops Password Auditor: Report showing end users with known compromised passwords*

Download Specops Password Auditor today: Get my free auditing tool

# Exposing the hidden risk of compromised passwords

It's important to have a password policy that blocks end users from creating weak passwords. But even strong passwords can become compromised through data breaches, phishing, and password reuse. Data from our 2023 Weak Password Report found that 83% of compromised passwords actually satisfied the length and complexity requirements of regulatory password standards such as NIST, HITRUST for HIPAA, ANSSI, PCI, and Cyber Essentials for NCSC.

New data we found from surveying 151 cybersecurity professionals at the 2023 International Cyber Expo event showed only 50% of organizations scan for compromised passwords more than once a month and 18% run daily scans. This leaves plenty of opportunity for attackers to exploit compromised passwords before they're rooted out by security teams.

## Compromised cloud application credentials

Modern organizations often use hundreds of cloud applications. New research from Outpost24's KrakenLabs team includes analysis of more than two million breached passwords from 81 of the most popular business applications used by HR, Customer Success, Marketing, and Development teams. These credentials were all stolen by malware and offer back doors for hackers looking for company information outside of the network. As if a hacker is unable to gain unauthorized access an organization directly, they might try to access a service used by that organization.

The findings highlight a major cybersecurity weakness where employees could use weak or previously leaked passwords for these services, often with little or no strong authentication in place. All of the below are real passwords that have been compromised by malware along with usernames, making it easy for attackers to log into the relevant cloud apps. As you can see, these applications have allowed the use of weak and commonly reused passwords that would be rapidly guessed in a brute force or dictionary attack:

| Cloud application password | Times found |
|---|---|
| 123456 | 1,459,484 |
| admin | 1,415,481 |
| 12345678 | 543,203 |
| password | 248,738 |
| 000000 | 91,395 |
| Admin123 | 73,711 |
| Password | 60,123 |
| user | 53,578 |
| Pass@123 | 54,781 |
| P@ssw0rd | 49,002 |

These are concerning results, considering the cloud applications in question contain all manner of sensitive data and business-critical operations instead. It's interesting to note passwords like Pass@123 and P@ssw0rd that would pass Active Directory's basic built-in rules were prevalent, highlighting the increased risk of password reuse for organization's not implementing strong password controls. An end user's Active Directory password could be at risk if they're reusing it on cloud applications that are vulnerable to credential theft by malware.

The KrakenLabs team also grouped applications by department (Development, Security, Marketing/Sales, HR, and Customer Success) to run some comparisons between relative password strength. For this research, a simple scoring method for assessing password strength was used. They looked at length, complexity (mix of lower case, upper case, number, and symbol), and entropy (measure of predictability, essentially complexity + length). The results weren't wildly different, but Development and Security teams had slightly stronger passwords. Customer Success applications had the weakest passwords by all counts.

**Average compromised password length:**

- Development (12)
- Security (11.8)
- Marketing/Sales (11.75)
- HR (11)
- Customer Success (10.2)

**Average compromised password complexity:**

- HR (3.84)
- Development (3.47)
- Security (3.42)
- Marketing/Sales (3)
- Customer Success (2.61)

**Average compromised password entropy:**

- Development (3.24)
- Security (3.16)
- HR (3.16)
- Marketing/Sales (3.1)
- Customer Success (3)

These results highlight that no department is safe from the risk of passwords becoming compromised and all users need to be protected. The research also suggests that a required Active Directory password length of at least 13 would greatly reduce the danger of cloud application password reuse in Active Directory environments. However, it's important to understand why even long passwords aren't totally safe and IT departments need to block the use of known compromised passwords in Active Directory.

## Are longer passwords safe from compromise?

Longer passwords are recommended as they're harder to guess and crack through brute force and hybrid dictionary attacks. Our 2023 Weak Password Report backed this up by finding 88% of passwords used to attack RDP ports in live attacks were 12 characters or less. As a further piece of research, our team analyzed an 800 million subset of the 4 billion unique compromised passwords within the Specops Breached Password Protection service.

As shown in the below list of descending order, the most common length for compromised passwords we found was 8 characters (212.5 million total compromised passwords were 8 characters exactly). As you can see, the rough rule of thumb is compromised passwords are more commonly shorter.

1. 8
2. 10
3. 9
4. 11
5. 12
6. 13
7. 14
8. 15

In the below table, we analyzed longer passwords (defined as over 12 characters in this case). You can see that as character length increases, the total amount of compromised passwords decreases. However, this doesn't mean we're talking insignificant numbers. Our team still found 31.1 million compromised passwords over 16 characters in length – and bear in mind this was from a smaller subset of our full database.

## Password Character Length in Compromised Passwords

| Character Length | Number of Compromised Passwords |
|---|---|
| > 12 | 121.5 million |
| > 13 | 90.3 million |
| > 14 | 67.7 million |
| > 15 | 45.7 million |
| > 16 | 31.1 million |

Below are the three most common compromised passwords for each of the character lengths we analyzed between characters lengths 8-15. There are some interesting things to dig into, especially at either end of the table. It comes as no surprise to see 'password' as the most commonly compromised 8-character password. The phrase 'new hire' appears in the second and third most commonly compromised 15-character passwords, highlighting that IT admins should avoid predictable, repeatable password patterns when onboarding new users. It could also suggest these new users were not forced to change their password and had been using the default ones given to them by IT for some time.

## Most Commonly Compromised Passwords By Character Length

| Character Length | Three Most Commonly Compromised Passwords |
|---|---|
| 8 | password<br>research<br>GGGGGGGG |
| 9 | GGGGGGGGG<br>anandIGBZ<br>cleopatra |
| 10 | OOOOOOOOOO<br>GGGGGGGGGG<br>passwordGG |
| 11 | Sym_cskill<br>sym_cskillO<br>FoxracingII |
| 12 | sym_cskillOT<br>sym_cskillOG<br>sym_cskillOB |
| 13 | mcafeeptfcorp<br>CitrixTargusl<br>rubyflankerG |
| 14 | hacktheplanetl<br>trendmirco.com<br>minecraft.A.S |
| 15 | SY&custskillsIO<br>Sym_newhireOEIE<br>sym_newhireOAIE |

We'd still always recommend organizations force end users to create longer passwords as they're harder to crack compared to shorter passwords. But this research highlights the fact that longer passwords can still become compromised – and often are. Relying on password length alone isn't enough, and additional security measures such as multi-factor authentication and continuous monitoring for compromised passwords should also be implemented.

## Can encrypted passwords still be hacked?

The Specops research team also conducted a study to see how long it would take for modern attackers to crack hashed passwords using brute force methods. Hashing algorithms are one-way functions that convert passwords into unique hash values, so to crack a hashed password, an attacker essentially needs to guess the original password.

Based on a hypothetical setup that a modern attacker could easily attain, our researchers created a table showing the estimated time it would take to crack passwords hashed with MD5. This is a relatively old hashing algorithm, but it's commonly used and appears in the most leaks as per the Have I Been Pwned 'Pwned website' list.

As shown below, short and non-complex passwords are still very easy to crack. Eight character passwords (even complex ones) can be cracked in under three hours. Compare that to complex passwords over 12 characters in length, which are essentially impossible to crack – even with MD5 which is considered a slightly less secure hashing algorithm than others.

## TIME TO CRACK: MD5 Hashed Passwords

| Number of characters | Numbers Only | Lowercase Only | Upper and Lower Case | Number, Upper, Lower | Number, Upper, Lower, Symbols |
|---|---|---|---|---|---|
| 8 | Instantly | Instantly | 2 minutes | 5 minutes | 3 hours |
| 9 | Instantly | 9 seconds | 2 hours | 5 hours | 12 days |
| 10 | Instantly | 4 minutes | 2 days | 14 days | 3 years |
| 11 | Instantly | 2 hours | 132 days | 3 years | 279 years |
| 12 | Instantly | 2 days | 19 years | 159 years | 26.5k years |
| 13 | Instantly | 6 weeks | 995 years | 10k years | 3m years |
| 14 | 3 minutes | 3 years | 51k years | 608k years | 239m years |
| 15 | 26 minutes | 82 years | 2m years | 37m years | 22.7b years |
| 16 | 5 hours | 2136 years | 140m years | 3b years | 3t years |
| 17 | 43 hours | 56k years | 8b years | 145b years | 205t years |
| 18 | 18 days | 2m years | 379b years | 9t years | 20q years |
| 19 | 6 months | 38m years | 20m years | 557t years | 2Q years |
| 20 | 5 years | 977m years | 2b years | 35q years | 176Q years |
| 21 | 49 years | 26b years | 54b years | 3Q years | 17s years |
| 22 | 490 years | 660t years | 3t years | 133Q years | 2S years |

*Time taken to brute force crack MD5 hashed passwords*

What about a more powerful hashing algorithm? The research team also put bcrypt to the test, which is considered stronger than MD5 due to its inclusion of salting (adding a random piece of data to each password hash). The algorithm also incorporates a “cost factor” that determines the number of password iterations and hashing rounds, further increasing the time and computational resources required to crack. Compared to older hashing algorithms like MD5 and SHA256, bcrypt proves to be significantly more secure against brute force attacks. As shown below, it’s still possible to crack short, non-complex passwords, but near-impossible once length and complexity are raised.

## TIME TO CRACK: bcrypt Hashed Passwords

| Number of characters | Numbers Only | Lowercase Only | Upper and Lower Case | Number, Upper, Lower | Number, Upper, Lower, Symbols |
|---|---|---|---|---|---|
| 6 | Instantly | 7 minutes | 7.5 hours | 22 hours | 11.5 days |
| 7 | Instantly | 3 hours | 16.2 days | 8 weeks | 3 years |
| 8 | 3 minutes | 4 days | 2.4 days | 9.5 years | 286 years |
| 9 | 23 minutes | 2.8 months | 120 years | 583 years | 27154 years |
| 10 | 3.8 hours | 6 years | 6228 years | 36160 years | 2579596 years |
| 11 | 38 days | 161 years | 323856 years | 2241941 years | 245061585 years |
| 12 | 15 days | 4169 years | 16840527 years | 139000337 years | 23280850.6 thousand years |
| 13 | 5.2 months | 15483 years | 875707453 years | 8618021 thousand years | 2211681 million years |
| 14 | 4.3 years | 2779344 years | 45536787 thousand years | 534317295 thousand years | 210109676 million years |
| 15 | 44 years | 72262968 years | 2367912 million years | 33127672 million years | 19960419.3 billion years |
| 16 | 431 years | 1878837183 years | 123131474 million years | 2053916 billion years | 1896240 trillion years |
| 17 | 4309 years | 48849767 thousand years | 6402837 billion years | 127342773 billion years | 180142784 trillion years |
| 18 | 43084 years | 1270094 million years | 332947505 billion years | 7895252 trillion years | 17113565 quintillion years |
| 19 | 430840 years | 33022443 million years | 17313271 trillion years | 489505617 trillion years | 1625789 quadrillion years |
| 20 | 4308396 years | 858583501 million years | 900291 quintillion years | 30349349 quintillion years | 154449919 quadrillion years |

*Time taken to brute force crack bcrypt hashed passwords*

However, it's important to note that while hashing provides a strong defense against password cracking, it cannot prevent password compromise if the passwords have already been exposed in data breaches. Password reuse remains a major risk, as attackers can steal passwords from less secure websites to gain unauthorized access to more secure systems. As shown in the below table, a compromised password takes no time to crack. Blocking the use of known compromised passwords will always be an essential part of defending against password guessing attacks.

## TIME TO CRACK: Known Compromised Passwords

| Number of characters | Numbers Only | Lowercase Only | Upper and Lower Case | Number, Upper, Lower | Number, Upper, Lower, Symbols |
|---|---|---|---|---|---|
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 8 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 9 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 10 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 11 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 12 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 13 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 14 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 15 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 16 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 17 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 18 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 19 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 20 | Instantly | Instantly | Instantly | Instantly | Instantly |

## Specops analysis: Why is password reuse such a threat?

Password reuse is a serious problem, but it's one organization don't always think about. Let's say you have a strong password policy in place that forces end users to pick a 15-character passphrase. Problems arise when an end user then takes this strong password and reuses it outside of work on their personal device on any site or app that requires a password. If an attacker obtains a database of passwords from one of these less secure sites, they can identify end users and try these credentials to gain access to their places of work. It only takes an end user one reuse of a work password to put their organization at risk.

It's estimated organizations using SaaS apps have an average of 47,750 passwords to manage, with 53% of people admitting to using the same password across multiple accounts. This creates a lot of potential for compromise. To protect against password reuse, organizations can provide training, implement multi-factor authentication, or get rid of passwords altogether (although this isn't a realistic option for most).

But the most effective method is using software that can continuously scan your Active Directory for compromised passwords and enforce change if an end user's password is found to have been involved in a breach.

*– Darren James, Senior Product Manager*

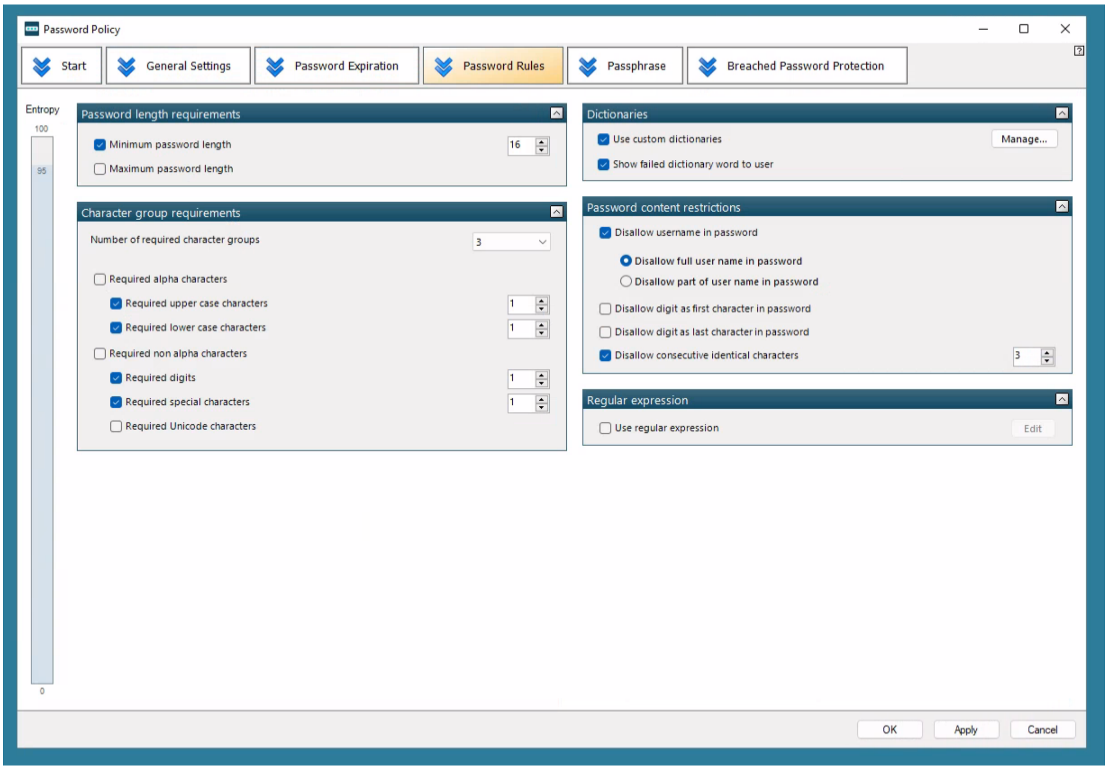
# How to block weak and compromised passwords

The data we've seen in this report highlights the need for stronger password policies, including the use of breached password lists and custom dictionaries, to prevent the use of common and easily guessable passwords. On top of that, organizations need a process in place to detect compromised passwords – even those that have become breached outside of the workplace. Here's how to achieve both steps and some tools that could help.

## Enforce a strong password policy

A password audit is a great first step for getting a snapshot of password-related vulnerabilities in your Active Directory – but you'll need a password policy to minimize risk on an ongoing basis. A tool such as Specops Password Policy can stop end users from creating weak passwords by blocking the following:

- Keyboard walk patterns such as 'qwerty' and '12345'
- Custom dictionary of terms specific to your organization. For example, you may want to block your company name, product names, or even local sports teams
- Passwords that don't meet your chosen customizable standard for length and complexity
- Any previously compromised password that's matched in our database of over 4 billion breached passwords
- And more!



Password length requirements

☑ Minimum password length 16

□ Maximum password length

Character group requirements

Number of required character groups 3

□ Required alpha characters

☑ Required upper case characters 1

☑ Required lower case characters 1

□ Required non alpha characters

☑ Required digits 1

☑ Required special characters 1

□ Required Unicode characters

Dictionaries

☑ Use custom dictionaries

☑ Show failed dictionary word to user

Password content restrictions

☑ Disallow username in password

● Disallow full user name in password

○ Disallow part of user name in password

□ Disallow digit as first character in password

□ Disallow digit as last character in password

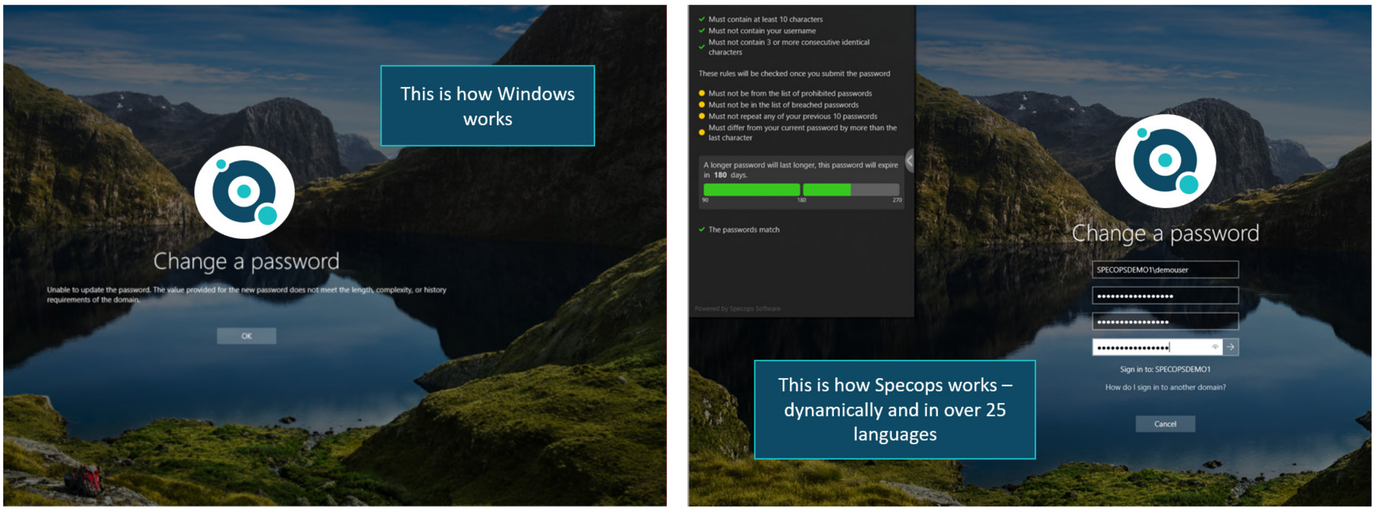
☑ Disallow consecutive identical characters 3

Regular expression

□ Use regular expression

*Specops Password Policy: Password policy settings*

A secure password policy alone won't be effective – end user experience matters too. Instead of a frustrating 'password doesn't meet criteria' message, Specops Password Policy offers dynamic feedback at the password-change screen which can help to guide your users to build a strong, memorable password. It also allows you to customize your end-user notifications. In addition, you have the option to offer length-based aging, which rewards users with more time before their next password reset when they choose a longer, stronger password.



This is how Windows works

Change a password

Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.

- ✓ Must contain at least 10 characters
- ✓ Must not contain your username
- ✓ Must not contain 3 or more consecutive identical characters

These rules will be checked once you submit the password

- ● Must not be from the list of prohibited passwords
- ● Must not be in the list of breached passwords
- ● Must not repeat any of your previous 10 passwords
- ● Must differ from your current password by more than the last character

A longer password will last longer, this password will expire in **180** days.

- ✓ The passwords match

Powered by Specops Software

Change a password

SPECOPSDEMO1\demouser

Sign in to: SPECOPSDEMO1

How do I sign in to another domain?

This is how Specops works – dynamically and in over 25 languages

*Windows password reset screen versus Specops Password Policy dynamic end user feedback*

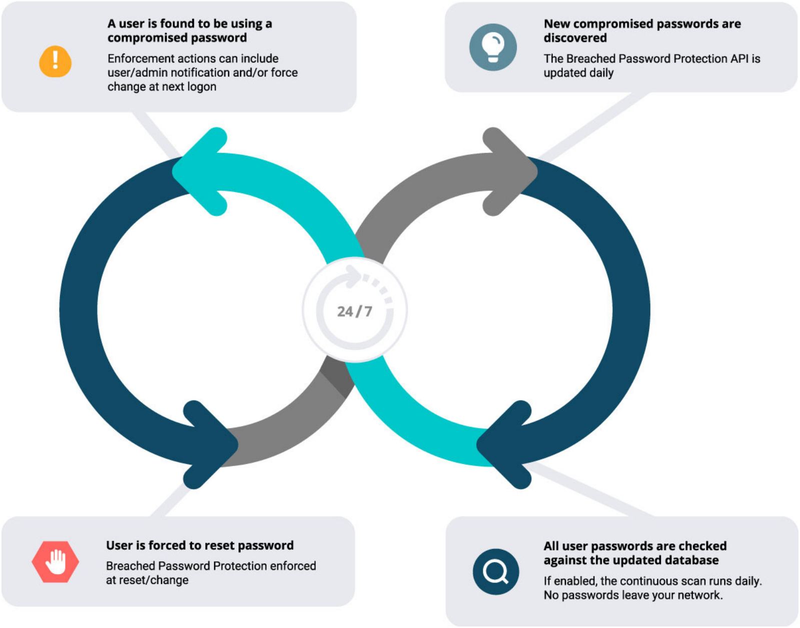
## Continuously scan for compromised passwords

Our data from surveying 151 cybersecurity professionals at the 2023 International Cyber Expo event showed 45% of organizations who only check for compromised passwords during expiry or reset events average only two checks for compromised passwords per year. This leaves them highly exposed.

Alternatively, the Specops Password Policy continuous scan feature provides daily checks against the Specops Breached Password Protection service, which is updated daily with passwords collected from honeypot networks, threat intelligence data, and newly discovered password leaks. This ensures that IT professionals have constant access to one of the most complete and up-to-date compromised password databases on the market.

By continuously scanning Active Directory passwords against the Breached Password Protection API, your IT teams can proactively identify compromised passwords within your organization. Continuous password scans can help detect potential security breach access points and enable prompt action to mitigate the risks associated with password reuse. It enables IT teams to automatically identify compromised passwords and immediately enforce the end user to change it at their next logon.

Incorporating the continuous scan feature into your password policy lets admins ensure compliance with industry best practices and regulatory requirements. The continuous scan results can be easily reviewed, giving a clear overview of compromised passwords within a network.


A user is found to be using a compromised password
Enforcement actions can include user/admin notification and/or force change at next logon
New compromised passwords are discovered
The Breached Password Protection API is updated daily
24 / 7
User is forced to reset password
Breached Password Protection enforced at reset/change
All user passwords are checked against the updated database
If enabled, the continuous scan runs daily. No passwords leave your network.

*Specops Breached Password Protection continuous scan feature*

Want to discuss how Specops Password Policy with Breached Password Protection could fit in with your organization? Reach out here.

SPECOPS
AN OUTPOST24 COMPANY

# About Specops

Specops Software, an Outpost24 company, is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. With a complete portfolio of solutions natively integrated with Active Directory, Specops ensures sensitive data is stored on-premises and in your control. Specops Software was founded in 2001 and is headquartered in Stockholm, Sweden with additional offices in the US, Canada, the UK, and Germany.