SpyCloud

Best Practices for Implementing NIST Password Guidelines

(NIST Special Publication 800-63B)

With Special Instructions for Active Directory

NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Best Practices Overview

Over the years, security professionals have learned surprising lessons about how password policies affect user behavior. As it turns out, strict password complexity rules and periodic forced password-change policies don't lead to stronger passwords. Instead, they make passwords harder for people to remember, encouraging dangerous shortcuts like choosing predictable passwords or reusing a few favorites across hundreds of accounts.

When users take shortcuts, cybercriminals benefit. Attackers systematically test credentials stolen from data breaches across other accounts, ranging from employers' Active Directory services to online service providers. With the help of sophisticated account checking tools, even unsophisticated criminals can automate credential stuffing and password spraying attacks at scale against a variety of targets.

For organizations, controlling users' bad password habits poses a major challenge. That's why the most recent password guidelines created by the National Institute of Standards and Technology (NIST) take human behavior into account. The latest guidelines, which are laid out in NIST Special Publication 800-63B, section 5.1.1.2, strike a balance between human-friendly policies that encourage strong passwords and strategies to help enterprises mitigate risk.

Aligning your enterprise's password policy with the latest guidelines from NIST can help encourage better password habits and reduce the risk of account takeover. You can enforce many of these guidelines through the built-in settings provided by most directory services, including Microsoft Active Directory. Only a few guidelines, such as determining whether passwords have been exposed in a third-party breach, require outside enforcement.

Use your directory service to enforce basic password guidelines

You can enforce basic password policies through most directory services, including Active Directory and Azure AD.

Enforceable in Active Directory:

- **8-character minimum**
- **64+ character maximum**
- **Allow special characters**
- **Limit failed login attempts**

NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Set an 8-character minimum

REQUIRED

NIST requires a minimum password length of at least eight characters. Passwords shorter than eight characters are easy for an attacker to crack, as SpyCloud's own password-cracking research demonstrates.

> *You can set this requirement in Microsoft **Active Directory** by drilling into Security Settings > Account Policies > Password Policy and selecting "Minimum password length." Set the number of characters to at least eight.*

Allow 64+ characters

IMPORTANT

NIST recommends allowing users to set passwords of at least 64 characters. Long passwords increase the cost for a criminal to crack an exposed password. Allowing a wide range of password lengths makes it possible for users to set long passphrases and encourages the use of password managers.

> *In **Active Directory**, Microsoft allows a maximum of 127 characters by default in Windows 10, though your mileage may vary in certain circumstances. For Azure AD, Microsoft allows a maximum of 256 characters.*

Allow (but don't require) special characters

IMPORTANT

NIST recommends allowing the use of Unicode and printing ASCII characters, including spaces. (Consecutive space characters may be replaced with a single space to help account for mistyping.) For organizations that opt to allow Unicode, NIST provides a reminder to normalize passwords before hashing.

While allowing 64+ characters is recommended rather than required, NIST prohibits truncating passwords. Instead, make sure you respect the password maximum rule you share with users. For example, if you inform your users that your maximum password length is 64 characters, don't just save the first 32 characters.

> ***Active Directory** allows most printing ASCII characters by default, but does not allow Unicode characters.*

NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Limit failed login attempts

REQUIRED

NIST requires organizations to limit failed login attempts, which can make it more challenging for an attacker to access your user accounts. In section 5.2.2, the guidelines specify that repeated login attempts should be restricted to "no more than 100," with additional suggested precautions to make sure an actual user doesn't get locked out. These options may include using a CAPTCHA, increasing the time someone has to wait after every failed login attempt, whitelisting IP addresses, and any other risk-based methods of flagging bad actors.

> *In **Active Directory,** you can limit failed login attempts by drilling into Security Settings > Account Policies > Account Lockout Policy and selecting "Account lockout threshold" (set to 100 or fewer). You may also want to set values for "Account lockout duration" and "Reset account lockout counter after," though NIST doesn't require specific values for these.*

Set human-friendly password policies

Because the latest NIST guidelines override decades-old beliefs about what makes a strong password policy, they provide significant coverage of what NOT to do. Follow these guidelines to avoid setting requirements that encourage users' bad habits.

NIST's human-friendly guidelines:

- **Don't require password complexity**
- **Don't force arbitrary password changes**
- **Don't use password hints or reminders**
- **Don't use knowledge-based authentication**

Don't require password complexity

IMPORTANT

NIST reverses older guidance by advising against requiring composition rules, such as using a combination of letters and symbols. In theory, using a mix of letters, numbers, and symbols can increase the difficulty of cracking a password. In practice, however, this type of requirement leads users to select shorter passwords that are challenging for them to remember, but easy for criminals to crack.

NIST

GUIDELINE LEVELS

REQUIRED (shall)

IMPORTANT (should)

DESIRABLE (may)

For example, a user can slip by most complexity requirements with a password like **'P@ssw0rd!'** Because the password follows the required composition rules, the user may assume they've made a secure choice. Unfortunately, criminals are well aware of the practice of applying 'leet speak' to a dictionary word or varying a password by a few characters to recycle it. Many account-checking tools test this type of password variation automatically. Even worse, the user may reuse variations of their 'secure' password choice across multiple services, exposing themselves to further risk.

*In **Active Directory**, you can disable password composition rules by drilling into Security Settings > Account Policies > Password Policy and selecting "Password must meet complexity requirements." Select "Disable."*

Don't force arbitrary password changes

IMPORTANT

NIST recommends avoiding arbitrary password changes, such as routine password expiration every 90 days. This type of requirement makes it harder for users to remember passwords and encourages bad habits such as choosing weak passwords, rotating through a set of familiar passwords, or 'updating' existing passwords with trivial changes.

Password rotation is a boon to criminals. When organizations enforce password expiration, criminals know that some users will inevitably cycle through older passwords, including those that have been exposed in previous breaches. That's one reason criminals will patiently test stolen credentials against other accounts over the course of months or years.

*In **Active Directory,** you can turn off password expiration and related settings by drilling into Security Settings > Account Policies > Password Policy and make the following changes:*

1. *Select "Set maximum password age" and set this to 0 to ensure that passwords never expire.*
2. *Select "Enforce password history" and set this to 0, which will allow users to use previous passwords. (While NIST does recommend prohibiting previously-breached passwords, it does not make a recommendation about restricting previous passwords.)*
3. *Select "Set minimum password age" and set this to 0 to remove limits on how often a user can change their password.*

NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Don't use password hints or reminders

REQUIRED

NIST advises against using any kind of password hint that an unauthenticated party could access, such as password hints or reminders. Users may underestimate the risk of providing too much information in a reminder field, which can make it easier for a criminal to guess the password and access the account. Some users will go so far as to set their actual password as the hint.

> *By default, **Active Directory** already doesn't support the use of hints and reminders.*

Don't use knowledge-based authentication

REQUIRED

NIST advises against knowledge-based authentication prompts, such as asking for the model of a user's first car. Often, these questions use information available through public records or social media. In addition, users may be prompted to answer the same questions across multiple services, encouraging credential reuse. If a criminal has access to other information about a user, this type of authentication may be easy to guess.

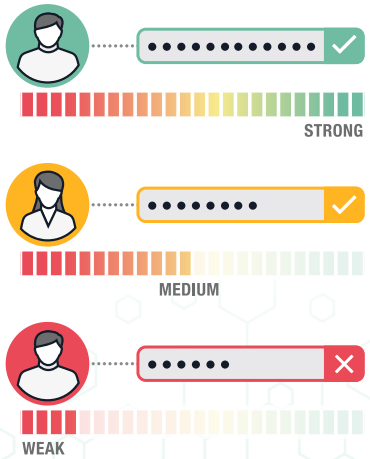
> *By default, **Active Directory** already doesn't support the use of knowledge-based authentication.*

Help your users help themselves

NIST offers usability guidelines that encourage users to select strong passwords, without directly implementing requirements. Some of these are available out-of-the-box with Active Directory, with the exception of providing password creation guidance such as a password-strength meter.

Active Directory Supports:

- **Offer the ability to view the full password**
- **Allow users to paste in passwords**
- **Password creation guidance**



NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Offer the ability to view the full password

IMPORTANT

NIST advises allowing users to select an option to view their full password, which can help them check their entry for errors. Optionally, NIST also suggests showing one character at a time as the user enters it to help mobile users avoid mistakes.

> ***Active Directory** provides the ability for users to display the full password by default.*

Allow users to paste in passwords

IMPORTANT

According to NIST, the ability to paste passwords "facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

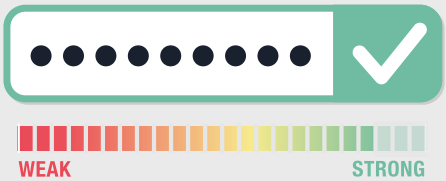
> ***Active Directory** provides paste functionality by default.*

Provide password creation guidance, such as a password strength meter

IMPORTANT

NIST recommends providing password strength guidance to users as they create a password, which might take the form of a password-strength meter.

> *A password strength meter is not available out of the box with **Active Directory.** Given that NIST classifies this guideline as important rather than required, organizations using Active Directory may choose to forgo this recommendation or include password strength reference materials or education to employees. Alternatively, your organization can evaluate the integration of a third-party tool for this purpose. For example, this is a feature of most password managers.*



NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

Ban "commonly-used, expected, or compromised" passwords

REQUIRED

NIST requires organizations to identify "commonly-used, expected, or compromised" passwords and, if selected, force users to reset them. According to NIST, these include, but are not limited to:

> - ***Passwords obtained from previous breach corpuses.***
> - ***Dictionary words.***
> - ***Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').***
> - ***Context-specific words, such as the name of the service, the username, and derivatives thereof.***

Aided by uses' bad password habits, criminals actively use these types of common and compromised passwords in account takeover attacks. Of the 53,000 security incidents covered in the 2018 Verizon Breach Report,[1] 48 percent involved stolen credentials.

Following NIST guidance to restrict usage of weak or exposed passwords is the best thing organizations can do to protect themselves. However, you likely won't get this functionality out-of-the box from your directory service. Here are a few best practices to help you comply with NIST's guidelines.

Check your users' passwords against an evolving list

Comparing passwords to a static list will not satisfy NIST's guidance. New breaches happen all the time, continually adding to your organization's risk exposure. To provide a sense of scale, SpyCloud researchers add about a billion new breach assets to our database every month.

It's not reasonable for most security teams to research and operationalize high volumes of breach data on their own. Organizations without a dedicated team to support this effort should evaluate vendors who can help. As you evaluate solution providers, look for a provider that collects new breach data regularly and provides a large database of plaintext passwords for you to check against your own user passwords. Also consider how the provider helps you put that data to use.

Ask potential solution providers:

- **How often do you identify new breaches?**
- **How large is your database of breach records?**
- **How large is your database of plaintext passwords?**
- **How do you make breach data actionable for organizations?**
- **How do I use your solution to check for weak or exposed passwords?**
- **Do you offer a way to reset weak or exposed passwords automatically?**

SpyCloud Tip

Put vendors to the test

The best way to evaluate a potential solution is by putting it to work through a proof of concept, or a head-to-head "data test" if you're comparing more than one vendor.

NIST

GUIDELINE LEVELS

- **REQUIRED (shall)**
- **IMPORTANT (should)**
- **DESIRABLE (may)**

SpyCloud Tip

Look for the cracks

Avoid providers that don't crack passwords, which either indicates that their data is not actionable for you, or that they collect data late in the breach timeline.

Get access to new exposures as soon as possible after a breach

By the time a data breach makes headlines, the worst damage has already been done. During the first 18 to 24 months after a breach, criminals restrict access to a close group of associates while they crack passwords and systematically monetize the stolen credentials. This is the most lucrative time for a criminal to have access to stolen credentials, and the most dangerous time for enterprises. Once the exposed logins begin to trickle onto deep and dark web forums where anyone can access it, their value drops substantially and they become low-value commodities.

It's critical to identify stolen credentials early in the breach timeline, when they are highly valuable to criminals and pose substantial risk to your enterprise. The only way to capture the data at this point is by infiltrating criminal groups using human intelligence techniques. To best protect your organization, find a provider who uses human intelligence to collect exposed credentials early, when they pose the greatest risk to your enterprise.

Ask potential solution providers:

- **How early in the breach timeline do you typically identify new breaches?**
- **What methods do you use to find breach data?**
- **Do you use human intelligence (HUMINT) to collect breach data?**
- **Do you crack passwords, or do you collect passwords that have already been cracked by criminals?**

Think from the criminal's perspective

Checking user passwords for dictionary words, repeated characters, and exposed passwords is an important step. However, you should consider other ways that criminals commonly exploit users' bad password hygiene to weaponize password lists.

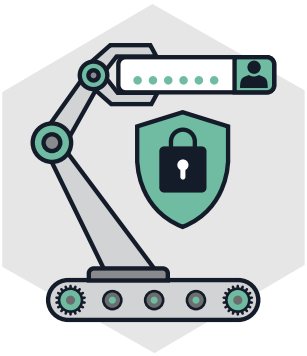
Often, people reuse passwords with minor variations, such as adding an exclamation point to or a number. Because of outdated password complexity requirements, users often assume that a password like "Spr1nkles!" is a secure password. Criminals use this. When credentials from your organization appear in a third-party breach, criminals can easily find both exact and "fuzzy" matches with common variations using automated account-checker tools.

Users' personal accounts also create a common blind spot for security practitioners, who typically have no way of knowing whether an employee has reused their work password with personal usernames. For an attacker, on the other hand, it's easy to connect an exposed password for john.smith@gmail.com to their corporate account, john.smith@employer.com.

NIST

GUIDELINE LEVELS

- REQUIRED (shall)
- IMPORTANT (should)
- DESIRABLE (may)



Ask potential solution providers:

- Can you check for both exact and "fuzzy" variations of exposed credentials?
- Can you check against all exposed passwords in the provider's database?
- Can you check for corporate passwords that have been exposed by personal accounts or other usernames?

Establish essential security controls

Generate secure PINs

REQUIRED

If you ever generate pins or passwords on behalf of your users, NIST requires that they be at least 6 characters long and "generated using an approved random bit generator" as described in NIST Special Publication 800-90A.

Encrypt passwords during transmission

REQUIRED

NIST requires that you "use approved encryption and an authenticated protected channel" when transmitting user passwords to reduce the risk that a third party might intercept your users' passwords.

To secure your employees' login credentials, be sure that your network is secure and requires a login credential. If your network communication is not secure, anyone who connects can see its traffic. When login information is sent, anyone watching can see the password in plaintext. For external users, make sure that your login portal has a valid SSL certificate to ensure network communication is encrypted.

Salt and hash stored credentials, including a keyed hash

REQUIRED

NIST provides specific guidelines for salting and hashing stored credentials.

To summarize, you should:

- ✓ **Pick a modern hashing algorithm (PBKDF2, bcrypt, etc.) that is resistant to decryption efforts**
- ✓ **Pick a long enough salt for each hash**
- ✓ **Make sure that the particular hashing algorithm is also using a pepper**

Delving into hashing methodologies is beyond the scope of this whitepaper. However, you can read SpyCloud research on the importance of choosing a modern hashing algorithm and the value of using salts and peppers to understand the implications of your choices.

Simplify NIST Password Guidelines with SpyCloud

Most NIST guidelines can be enforced using the built-in controls in directory services like Microsoft Active Directory. However, the list of exposed passwords evolves constantly as new breaches emerge. For busy security teams, keeping up with the latest breach data and applying it to user credentials poses a major challenge.

This is exactly where a solution like SpyCloud can help. SpyCloud helps enterprises align with NIST password guidelines by checking user passwords against the largest database of stolen credentials in the world. With over 100+ billion recovered breach assets to date, and 1 billion more added every month, enterprises can integrate SpyCloud's breach data into their SIEM, Active Directory, and internal custom applications with fast, high-volume access. SpyCloud enables remediation when it really counts — before criminals have illegitimately accessed corporate systems and data or siphoned off cash & loyalty points from consumer accounts.

With **SpyCloud Active Directory Guardian,** enterprises can easily operationalize SpyCloud's data to automatically detect and reset Active Directory passwords NIST would classify as "commonly-used, expected, or compromised," including passwords exposed in breaches and a pre-populated "banned password" list. For added assurance, Active Directory Guardian makes it possible to check Active Directory passwords against every password in SpyCloud's database using k-anonymity, independent of username. Active Directory Guardian does not need to run on the domain controller, enabling you to remediate exposed passwords with minimal risk to your organization.

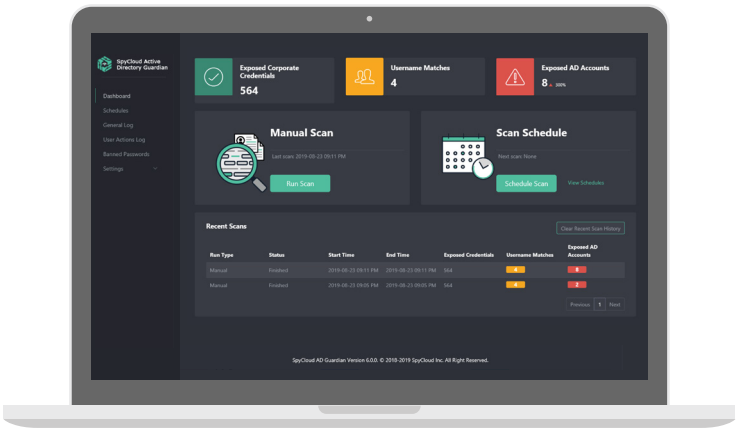


Figure 1: Spycloud's Active Directory Guardian Dashboard

Given the NIST guidelines, a solution like SpyCloud is key to an enterprise's efforts to combat account takeover.

SpyCloud