2022

A VMsources Whitepaper

Simple and cost-effective security: Password Policy

JOHN BORHEK / VMSOURCES

Contents

Introduction

Last week, as I was logging into an often-used site, I was prompted to create a new password because mine had expired. The new password needed to be at least 8 characters containing “one Uppercase, one lowercase, one number, and one special character.” Basically, the IT admin of the site was telling me: “Please write your password on a post-it and stick it to your monitor!.”

While it’s not exactly new news, a remarkable number of people don’t know that the NIST has completely overhauled its password policy recommendations. The recommendations toss aside counter-productive requirements like password aging and mandatory complexity; instead favoring common sense like the use of passphrases and minimum password length.

Every day some company, organization or individual gets busted because there has been a data breach. Anytime data is compromised, it’s headline news around the world! Many incidents occur due to simple password exploitation. Like it or not, the username password combination is at the root of IT security, and used by all of us. Don’t become the next headline, because you failed to implement the latest guidelines by NIST!

I hope this helps, and encourage you to conform your password policy to **NIST Special Publication 800-63B**. While we may seek and implement other measures and 3rd party tools to improve authentication in our organizations – improved policy is the simplest and most cost-effective tool available. While implementing the latest password policy guidelines may not make your organization impervious, it will deflect any finger-pointing should a breach occur. Wouldn’t you like to be able to say: “my company has fully implemented all of the latest recommendations from NIST!”

Sincerely,

John Borhek

John Borhek,
Lead Solutions Architect
Email: john@vmsources.com
Website: https://vmsources.com
Mobile: +1 928.606.0483
Office: +1 215.764.6442 X1001

Password recommendations is by NIST

The **NIST issued Special Publication 800-63B**, debunking many of the counterproductive policies foisted upon us by auditors and administrators concerned more with the "letter-of-the-law" that actual security.

The DOs and DONTs:

The NIST uses the unambiguous terminology of "SHALL" and "SHALL NOT" in Special Publication 800-63B. In this article, I have attempted to distill the NIST recommendations to those points which **apply directly to Kerberos based user directories such as Active Directory.** Many of the recommendations below are directly contradictory to current policies and should be updated immediately.

Don't forget, if you are running vCenter, you have a separate Kerberos directory known as vSphere SSO. Your SSO Directory contains at least one user, and those policies should be updated concurrently with AD to meet NIST guidelines.

The DO's

- **DO use multi-factor authentication**
- NIST Says (4.2.1) authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.
- **DO allow use of passphrases**
- NIST Says (5.1.1.2): "Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets."
- **DO allow the use of cut & paste for passwords**
- NIST Says (5.1.1.2): "Verifiers SHOULD permit claimants to use "paste" functionality when entering a memorized secret."
- **DO favor users, not administrators**
- NIST Says (6.1.3): "password policies should be user friendly and put the burden on the verifier"
- **DO enforce password length**
- NIST Says (5.1.1.1) "Memorized secrets SHALL be at least 8 characters in length"
- **DO create a banned-list and compare passwords to known-bad passwords**
- NIST Says (5.1.1.2): "compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised"

- **DO enforce timeout for inactivity**

- NIST Says (4.3.4): “Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 15 minutes or longer”

- **DO allow users to see their passwords in plain text**

- NIST Says (5.1.1.2): “offer an option to display the secret — rather than a series of dots or asterisks — until it is entered”

The DO NOT’s

- **DO NOT require numbers, special characters or enforce composition rules**

- NIST Says (5.1.1.2): “Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.”
- **DO NOT use hints or questions**

- NIST Says (5.1.1.2): “Memorized secret verifiers SHALL NOT permit the subscriber to store a “hint” that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., “What was the name of your first pet?”)
- **DO NOT enforce password aging**

- NIST Says (5.1.1.2): “Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”