Improving Security and the User Experience: Discontinuing Password Expiration

Overview

Password expiration is the process in which passwords are required to be changed after a specific periodic of time. As an example, Cisco requires employees to change their passwords every 180 days. While password expiration has been widely accepted as a security best practice in most organizations, this process is no longer considered a control that reduces risk.

Over 90% of compromises are attributed to social engineering initiated via an enticing email, website or link that results in malware being installed on a user's device to access passwords. As passwords can be captured in real-time, frequent rotation does not prevent accounts from being compromised.

The U.S. National Institute of Standards and Technology (NIST) organization has recently changed their perspective on password management and has published updates to their Digital Identity Guidelines. In adherence to these revised standards, Cisco is discontinuing password expiration to access information systems.

How Cisco Improves Security and the User Experience

What is Cisco's current password management protocol?	• Cisco currently requires users to change their password every 180 days. • Users are required to authenticate via multi-factor authentication (MFA) to access network resources.
What is Cisco implementing to improve user password and device security?	• Adopting NIST Standards and eliminating password expiration. • Enforcing the use of certificates for the 1st factor instead of passwords. • Enforcing the use of MFA on all applications for the second factor. • Leveraging User Behavior Analytics (UEBA) to detect and alert on anomalous authentication events that can lead to potential account compromise. • Leveraging device posture checks to ensure all end points meet a minimum-security bar for application authentication.

What are the benefits of discontinuing password expiration?	• Improved security and decreased risk of compromised user accounts. • Improved experience as users won't have to reset and remember new passwords. • Increased productivity by removing administrative burden of resetting and managing passwords. • Reducing friction associated with reinforcing password expiration requirements.
What should a user expect in terms of experience?	• For access to certain resources, users will still be required to input a password and authenticate via MFA. • Users can continue using their existing password credentials. • Users will stop receiving email notifications about needing to change their password every 180 days.
Is there anything I should know or do as a result of this new protocol?	• The discontinuation of password expiration will be effective on September 29, 2021. • If anomalous activity is detected through UEBA, users will automatically receive a security alert requiring action and they will be directed to verify authentication activity. If credentials have been compromised, users will be prompted to re-set their password.
What kind of password accounts does this apply to?	• Eliminating password rotation applies to human accounts and does not apply to generic, service or privileged accounts.
How can I learn more about the NIST Standards regarding passwords?	• Information regarding updates to Digital Identity Guidelines can be found in this NIST Special Publication 800-63B
Where can I access information that addresses these policy changes?	• Information regarding Cisco's authentication policies can be found in this Data Brief.