ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Refining Password Policies within IBM's Sterling Integrator for Enhanced Managed File Transfer Security

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA

ABSTRACT

Robust password policies are crucial for securing Managed File Transfer (MFT) systems. IBM's Sterling Integrator, a leading platform in MFT, necessitates stringent password protocols to mitigate cyber threats. This paper proposes an enhanced password policy framework for Sterling Integrator, focusing on balancing security requirements with user experience. By integrating advanced authentication mechanisms and leveraging user psychology, we aim to fortify MFT security without compromising usability.

***Corresponding author**

Prashanth Kodurupati, Information Technology, Managed File Transfer Engineer, PragmaEdge LLC, Alpharetta, USA.

Received: June 10, 2022; **Accepted:** June 15, 2022; **Published:** June 24, 2022

Keywords: IBM Sterling Integrator, Password Policies, Managed File Transfer, Cybersecurity, User Experience

Introduction

Despite how COVID-19 has halted almost every aspect of the world, unfortunately, cybercrime has risen considerably. Phishing incidents and brute-force password hacking has become a major concern, with a rise of 220% being reported throughout the year. In such an environment, organizations and government bodies are actively trying to mitigate these threats.

However, the leading cause of brute-force attacks being popularized is the fact that many individuals tend to use passwords that are convenient and quick to use. These may either be all numbers, all same-case letters, or even their own names.

The environment around password policies has constantly been evolving as cyberattacks become more and more sophisticated. Organizations are constantly facing a rising risk of unauthorized access to their systems. One of the leading causes for this is weak passwords.

High profile data breaches have recently come to light, such as the Marriot Data Breach on March 31st, 2020. The breach impacted more than 5.2 million guests. According to the press release, the breach was caused by a hacker who obtained passwords of two Marriot employees [1].

IBM's Sterling Integrator has become a staple for many organizations for internal and external communications, as a result. It is a B2B integration solution that provides a secure and seamless data exchange tool for electronic data interchange (EDI), file transfers, and other processes. However, it also requires strict password policies to be implemented for the sake of security. This, in turn, means a poor user experience for all.

This paper provides an in-depth analysis of this policy, its implementation challenges, and its impact on Managed File Transfer (MFT) processes.

Literature Review

The literature surrounding password policies and cybersecurity underscores the delicate balance between securing Managed File Transfer (MFT) systems like IBM's Sterling Integrator and ensuring user compliance and experience. Gontovnikas (2020) highlights the urgency of addressing cybersecurity threats, noting significant breaches and their impact on user data integrity [1].

Gunasinghe and Bertino (2018) propose biometrics and user-centric protocols as alternatives to traditional password systems, aiming to enhance security while reducing user inconvenience [2].

Problem Statement – Poor Usability for Improved Security

While Sterling Integrator's custom password policy introduces robust security measures, it presents several challenges:

User Compliance and Experience

The Sterling Integrator's custom password policy, while enhancing security, mandates the use of complex passwords that combine upper and lower case letters, alphanumeric characters, and forbids identical consecutive characters [3]. Such stringent requirements can lead to frustration among users, particularly when creating new passwords or updating existing ones.

The policy's focus on complexity can deter user compliance, as individuals may struggle to remember their passwords, potentially leading to increased support calls for password resets and decreased overall productivity.

Implementation Complexity

To activate the custom password policy, administrators must implement custom Java code through a designated plug-point. This process requires a deep understanding of the Sterling

Integrator's architecture and Java programming, posing a barrier for organizations with limited technical resources [4]. The necessity for specialized expertise not only increases the time required to deploy the policy but also elevates the risk of errors during implementation, which could inadvertently weaken the system's security posture.

Integration Hurdles

The custom password policy applies exclusively to internal user accounts. For organizations that rely on Lightweight Directory Access Protocol (LDAP) for external account management, this limitation hampers the uniform application of security measures across all user accounts [4]. The inability to enforce the custom password policy on LDAP-managed external accounts creates a security inconsistency, leaving a portion of the user base less protected than others.

Lack of Security and Usage Balance

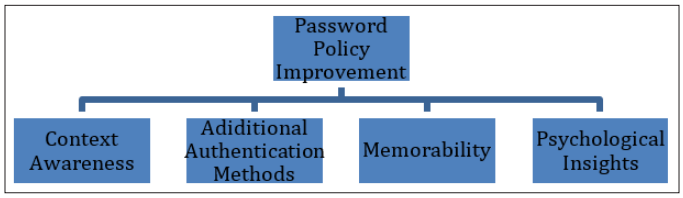
The ultimate challenge lies in striking an optimal balance between imposing rigorous security measures and maintaining a user-friendly system. Overly complex passwords can enhance security but at the cost of usability, leading to potential resistance from users [4]. Finding a middle ground where password policies are both secure and user-friendly is critical for encouraging compliance and ensuring the system's effectiveness.

Academic Review of Key Challenges and Proposed Solutions

Research	Challenge	Solution
Gontovnikas (2020)	Rising cybersecurity threats and data breaches	Enhanced security protocols and awareness
Chandrasiri (2017); Ur et al. (2017)	Balance between password strength and memorability	Integrating user psychology into policy design
Bullo (2017)	Lack of user situational awareness	Transparent, context-aware password policies
Woods, Siponen (2019)	Difficulty in remembering complex passwords	Policies that improve password memorability

Proposed Solution: Adaptive Security Framework (ASF)

Considering the large number of threats that consumers have to deal with every day, the need for password policies remains astute. To ensure that the policies maintain a user-friendly approach, there are four critical elements that can implemented [3];



1. Maintaining context awareness,
2. Implementing additional user-authentication methods,
3. Ensuring memorability in the system to reduce password input every time
4. Using psychological insights with policies.

The proposed solution focuses on the psychological aspect of consumers, while ensuring cybersecurity in a convenient manner when using IBM's Sterling Integrator for MFT purposes [3].

Dynamic Password Policy Adjustment

The ASF would utilize Sterling Integrator's extensible architecture to implement dynamic password policy adjustments. By assessing contextual factors such as the user's role, location, and the security posture of the device being used for access, the ASF would tailor password requirements in real-time [2].

For instance, access from a company-secured device within the corporate network might necessitate simpler passwords compared to access attempts from unknown devices or public networks. This approach ensures that security measures are proportionate to assessed risk levels, enhancing user compliance without compromising security [2].

Modular Designs for Implementation

To minimize the implementation complexity, the ASF can be designed as a series of modular components or plugins that can be easily integrated into Sterling Integrator's existing framework. These modules would interact with the system's plug-point for custom code integration, offering a library of pre-configured, customizable password policy templates.

This modular design reduces the need for in-depth custom coding and simplifies the deployment process, allowing organizations to quickly adapt to evolving security requirements.

Balanced Account Coverage

The ASF extends the adaptive password policies to both internal and external user accounts by integrating with LDAP systems through a secure API layer.

This ensures that the same dynamic security standards are applied uniformly across all user accounts, eliminating disparities in protection levels between internal and external users. The API layer facilitates real-time communication between Sterling Integrator and external directory services, enabling the ASF to apply context-sensitive password policies across the board [5].

At the heart of the ASF is the principle of balancing rigorous security measures with a positive user experience. This user-centric approach not only improves compliance rates but also enhances the overall perception of the system's usability. Users are less likely to circumvent security measures that are intelligently applied and that recognize the nuances of their individual access contexts [6].

Use Cases

In this use case, we demonstrate how an organization using IBM's Sterling Integrator can enhance its password security by implementing a custom password policy extension.

An organization has identified that despite having a password policy in place, users are still able to set weak passwords that do not meet the desired security standards. The goal is to enforce a stricter policy that mandates the use of both lowercase and uppercase characters, numeric digits, and special characters in passwords, without relying on the default Sterling Integrator settings.

Step 1: Configure the Custom Password Policy Extension

The first step involves declaring the custom password policy extension in the customer_overrides.properties file:
security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl

Step 2: Prepare the Development Environment
Head to the home directory: /home/IBM/SI/install. Then, create a new directory structure for the custom policy code: mkdir -p test/policy/extension.

The custom class PwdPolExtnImpl.java is created within the test/policy/extension directory with the following code:

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension {
    public String validateNewPassword(String pwd, String policyName) {
      // Additional password validation checks
      boolean match = Pattern.matches(".*[a-z].*", pwd) &&
                Pattern.matches(".*[A-Z].*", pwd) &&
                (Pattern.matches(".*[0-9].*", pwd) ||
                 Pattern.matches(".*[^A-Za-z0-9].*", pwd));
      if (match == true) return null;
      else return "nogood";
   }
}
```

Step 3: Next, Compile the Java class with the Sterling Integrator classpath. Use the following code to do so.

Compile the Java class with the Sterling Integrator classpath:

Step 4: Continue to package the compiled class into a JAR file and deploy it to Sterling Integrator:

```
cd /home/IBM/SI/install
jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class
./bin/install3rdParty.sh userExit 1_0 -j /home/IBM/SI/install/userExit.jar
```

After restarting the Sterling Integrator application, any new user account creation or password change will invoke the custom password policy.

Conclusion
To integrate the ASF within Sterling Integrator, a phased approach could be adopted. Initially, a pilot program involving a subset of users could be implemented to refine the ASF's functionality and ensure seamless operation with Sterling Integrator's current setup.

Feedback from this pilot phase would inform broader deployment, ensuring that the ASF meets the diverse needs of all users while upholding the highest security standards.

The custom password policy of Sterling Integrator is a pivotal element in securing B2B communications and MFT processes. By addressing the challenges associated with its implementation and user compliance, and proposing an adaptive security framework, this paper contributes to the ongoing dialogue on enhancing cybersecurity measures in complex digital environments. Future research should explore the integration of artificial intelligence and machine learning algorithms to further refine and automate the adaptive security framework, ensuring that Sterling Integrator remains at the cutting edge of secure B2B communications [7, 8].

References

1. Gontovnikas M (2020) The 11 Biggest Data Breaches of 2020 (So Far). Auth0 by Okta https://auth0.com/blog/the-11-biggest-data-breaches-of-2020-so-far/.
2. Gunasinghe H, Bertino E (2018) PrivBioMTAuth: Privacy Preserving Biometrics-Based and User Centric Protocol for User Authentication From Mobile Phones. IEEE Transactions on Information Forensics and Security 13: 1042-1057.
3. Chandrasiri HMSPK, Herath HMGC, De Wansa Wickremaratne JN (2017) Striking a balance between Password Strength and Memorability to Improve Information Security. Digital Library of University of Colombo School of Computing https://dl.ucsc.cmb.ac.lk/jspui/bitstream/123456789/3930/1/Group_2_Thesis.pdf.
4. Blase Ur, Felicia A, Maung A, Lujo B, Nicolas C, et al. (2017) Design and Evaluation of a Data-Driven Password Meter. 2017 CHI Conference on Human Factors in Computing Systems https://dl.acm.org/doi/10.1145/3025453.3026050.
5. Seitz T (2018) Supporting Users in Password Authentication with Persuasive Design. Munchen https://edoc.ub.uni-muenchen.de/22619/13/Seitz_Tobias.pdf.
6. Jeremiah B, Saranga K, Lorrie C, Anupam D (2020) Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords. Arxiv - Cornell University, Ithica, New York https://arxiv.org/pdf/1410.1490.pdf.
7. Bullo A, Eliana S, Stavros S (2017) Transparent password policies: A case study of investigating end-user situational awareness. University of Central Lancashire, Preston, Lancashire https://www.researchgate.net/publication/321152462_Transparent_password_policies_A_case_study_of_investigating_end-user_situational_awareness.
8. Naomi W, Mikko S (2019) Improving password memorability, while not inconveniencing the user. International Journal of Human-Computer Studies 61-71.