SWAMID template Password Policy

Purpose and Scope

This wiki page is SWAMIDs template Password Policy including password complexity and password guessing rate limiting. In this page there is an example in Swedish with an additional translation to English how to create an environment that establish a resonable security level to fulfil both SWAMID Identity Assurance Level 1 Profile and SWAMID Identity Assurance Level 2 Profile. For SWAMID Identity Assurance Level 3 Profile multi-factor login is used to establish a resonable security level and the password can be part one of the factors in a multi-factor login.

The Acceptable use Policy and the Password Policy could be merged into one Accept Use Policy.

Swedish template Password Policy

SWAMID template password policy is written in Swedish due to that the implementing organisation are Swedish legal entities.

Some reading help:

- The policy is made for a decentralised IT-organisation but is easily adapted to a centralised organization.
- All text within [] should be changed to local information.

Lösenordsregler

Detta dokument anger [ORGANISATION] policy för kvalitet på samt hantering av lösenord.

Som användare av [ORGANISATION] informationssystem ansvarar du själv för att

- dina lösenord uppfyller den kvalitet och hantering som anges i denna policy genom att
  - bestå av minst [ANTAL] tecken.
  - bestå av minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.
- du håller dina lösenord hemliga genom att
  - aldrig uppge dina lösenord till någon som efterfrågar dem via e-post, i telefon eller på annat sätt.
  - aldrig använda samma lösenord i andra system.
- du ändrar ditt lösenord om du fått kännedom om att säkerheten runt ditt lösenord har äventyrats.

English template Password Policy

SWAMID template password policy is written in Swedish due to that the implementing organisation are Swedish legal entities. The English template is a translation from Swedish.

Some reading help:

- The policy is made for a decentralised IT-organisation but is easily adapted to a centralised organisation.
- All text within [] should be changed to local information.

Password Policy

This document specifies [ORGANISATION] policy of quality and handling of passwords.

As a user of the computer systems at [ORGANISATION], you are yourself responsible for the following:

- your passwords fulfil the quality and usage described in this policy
  - consist of at least [NUMBER] of characters.

    - consist of at least one capital letter, at least one lowercase letter and either at least one special character or a number.
- you keep your passwords secret through
    - never give your passwords to anyone who requests them by email, phone or otherwise.
    - never use the same password in other systems.
- you change your password if you know it has been compromised.

Extra information on passwords quality

This information is not part of the password policy but is presented as informational material to interested parties.

Password complexity for user selected passwords

Password entropy as defined in (the old) NIST SP 800-63-2, Appendix A

Password entropy for user selected passwords is as follows for user-selected passwords drawn from the full US keyboard alphabet:

- The entropy of the first character is taken to be 4 bits;
- The entropy of the next 7 characters are 2 bits per character;
- For the 9th through the 20th character the entropy is taken to be 1.5 bits per character;
- For characters 21 and above the entropy is taken to be 1 bit per character;
- A “bonus” of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters.
- A "bonus" of up to 6 bits of entropy is added for an extensive dictionary check.
    - This "bonus" declines slowly as passwords gets longer and is at zero at 20 characters.

All SWAMID Assurance Identity Profiles requires at least 24 bits of entropy.

Complex passwords in Active Directory

If you in Active Directory enable complexity requirements policy for passwords, define a minimum password length, define rate limiting and define a maximum password age you can fulfil the proposed password policy.

Enabling the password complexity requirement policy setting requires new passwords to meet the following requirements:

1. Passwords may not contain the user's samAccountName (Account Name) value.
    - The samAccountName is checked in its entirety only to determine whether it is part of the password. If the samAccountName is less than three characters long, this check is skipped.
    - The check is not case sensitive.
2. Passwords may not contain the user's entire displayName (Full Name value).
    - The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed to not be included in the password. Tokens that are less than three characters are ignored, and substrings of the tokens are not checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.
    - The check is not case sensitive.
3. The password contains characters from three of the following categories:
    - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters).
    - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters).
    - Base 10 digits (0 through 9).
    - Non-alphanumeric characters (special characters) (for example, !, $, #, %).
    - Any Unicode character that is categorised as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Determining password strength

There are two factors to consider in determining password strength:

1. the average number of guesses the attacker must test to find the correct password and
2. the ease and speed of which an attacker can check the validity of each guessed password.

The first factor is determined by how long the password is, how large set of characters or symbols that be used in the password, if a combination of both lower, upper and non-alphabetic characters is used and whether the password is created randomly or created by the user himself. There is a trade of regarding demanding a high complexity and the user's ability to remember the password.

The second factor is the rate at which an attacker can submit passwords guesses to the system. If some kind of rate limiting and maximum password age is used the need for password complexity is greatly redused in online scenarios. However, the identity management system must store information about the user passwords in some form and if that information is stolen, say by breaching system security, the less complex passwords can be at greater risk.