Local Security Policy

Configuring Password Policy

- Password policy is a set of rules designed to enhance computer security by prompting the users to change passwords frequently and to select strong passwords.
- Password policy is often part of an organization's official regulations. It can be set depending on the needs of the organization.

The parameters that can be set for a password are:

- **Enforce password history**: Sets how frequently old passwords can be reused.
- **Maximum password age**: Determines how long users can keep a password before they have to change it.
- **Minimum password age**: Determines how long users must keep a password before they can change it.
- **Minimum password length**: Sets the minimum number of characters for a password.
- **Passwords must meet complexity requirements**: The password must include at least two opposite case letters, a number and a special character (punctuation marks, for example). Example qwe@123 which is a combination of letters, special characters and numbers.
- **Store password using reversible encryption**: Passwords in the password database are encrypted. This encryption cannot normally be reversed.

Configuring Account Lockout Policy:

- **Account lockout duration:**
  - sets the length of time the account is locked.
-
  - The lockout duration can be set to a specific length of time using a value between 1 and 99,999 minutes.

- **Account lockout threshold** :
  - sets the number of invalid logon attempts that are allowed before an account is locked out.

- **Reset account lockout threshold** :
  - after setting determines how long the lockout threshold is maintained. This threshold is reset in one of two ways.
-
  - If a user logs on successfully, the threshold is reset. If the waiting period for Reset account lockout threshold after has elapsed since the last bad logon attempt, the threshold is also reset.

APPLOCKER

Configuring AppLocker:

- AppLocker policies control applications by creating an allowed list of applications by file type.
- Exceptions are also possible.
- AppLocker policies can be applied only to the applications installed on computers running one of the supported versions of Windows.
- AppLocker contains new capabilities and extensions that allow you to create rules- to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications.

- The rules which can be created in Windows 8.1:

    - **Path rule:**

      The path condition identifies an application by its location in the file system of the computer or on the network.

      When creating a rule that uses a deny action, path conditions are less secure than publisher and file hash conditions for preventing access to a file because a user could easily copy the file to a different location than the location specified in the rule.

    - **Publisher:**

      Publisher conditions can be made only for files that are digitally signed; this condition identifies an app based on its digital signature and extended attributes.

      The digital signature contains information about the company that created the app (the publisher)

    - **Hash rule:**

      File hash rules use a system-computed cryptographic hash of the identified file. For files that are not digitally signed, file hash rules are more secure than path rules.

      Each time that the file is updated (such as a security update or upgrade), the file's hash will change. As a result, you must manually update file hash rules.