How To Customize A Local Password Policy in Windows 10/8/7

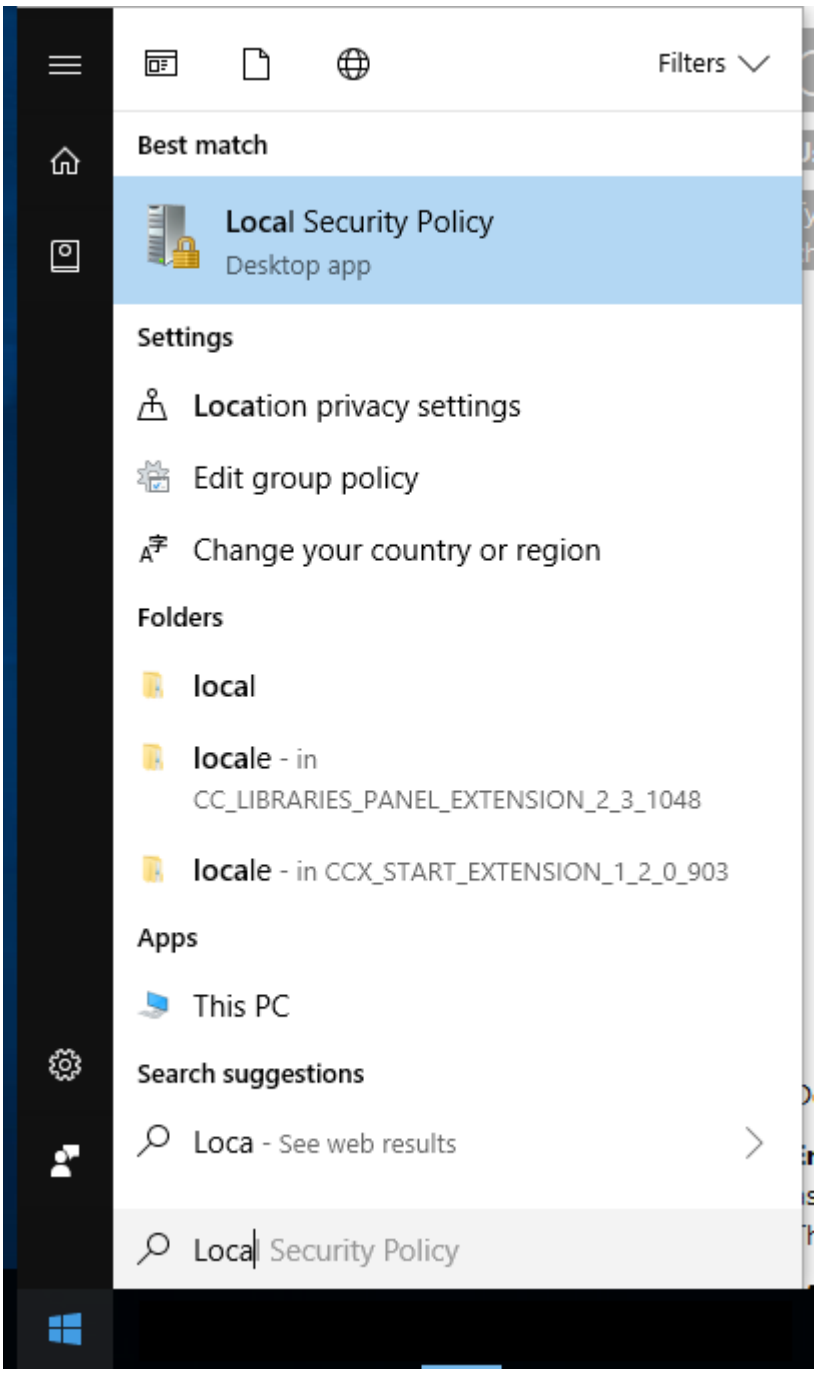
rdavis@foregenix.com - 2018-01-11 - Comments (0) - PCI Compliance

Setting A Windows Password Policy On Local (non-domain) Machines

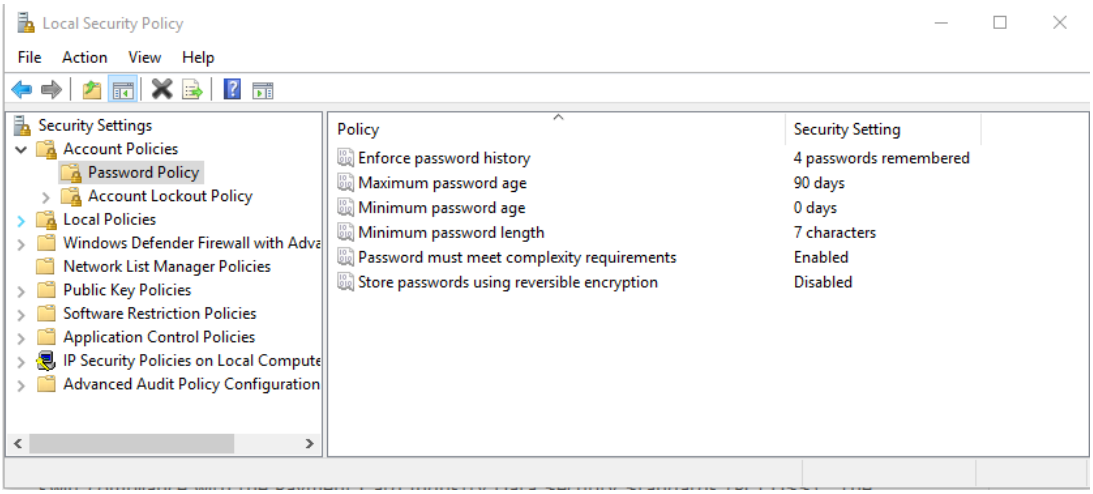
---

Using Local Security Policy.

Type Local Security Policy in the start menu search and press *Enter.* The LSP window will open. Now from the left pane, choose *Password Policy* from under *Account Policies.* Now on the right side six options will be listed.



This will start the LSP and you will see something like this, I have already set the minim needed to meet requirements:



Details of each of those options are listed below.

Enforce Password history: This security setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.

> **PCI Requirements:** Password parameters are set to require that new passwords cannot be the same as the four (4) previously used passwords.

Maximum password age: This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

> **PCI Requirements:** Users to change passwords at least every 90 days. It is recommened to use user a lower value here.

Minimum password age: This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0. The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.

PCI Requirements: No Requirements are set for this

Minimum password length: This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.

PCI Requirements: Require a minimum length of at least seven (7) characters.

Password must meet complexity requirements: This security setting determines whether passwords must meet complexity requirements. If this policy is enabled, passwords must meet the following minimum requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

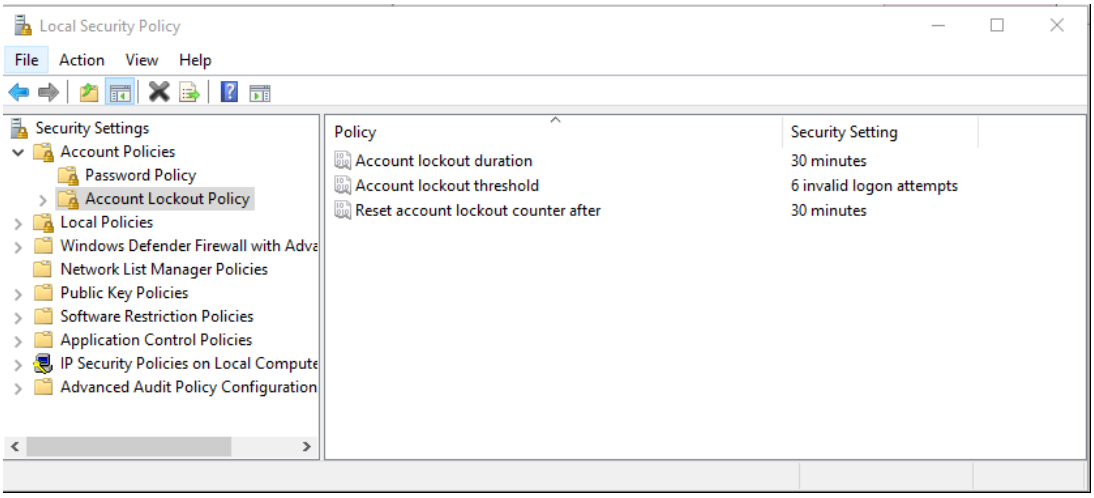
Complexity requirements are enforced when passwords are changed or created.

PCI Requirements: Contain both numeric and alphabetic characters. This must be enabled.

Store password using reversible encryption: This security setting determines whether the operating system stores passwords using reversible encryption. This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

PCI Requirements: Passwords are protected with strong cryptography during transmission and storage. This must be disabled.

The next step it to set the lock out policys, these have to be done in order:



Account lockout threshold: This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

> **PCI Requirements:** User accounts are temporarily locked-out after not more than six invalid access attempts.

Account lockout duration: This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

> **PCI Requirements:** Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. This will default to 30mins.

Reset account lockout counter after: This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

> **PCI Requirements:** This is not a defined requirement, but will default to 30mins.