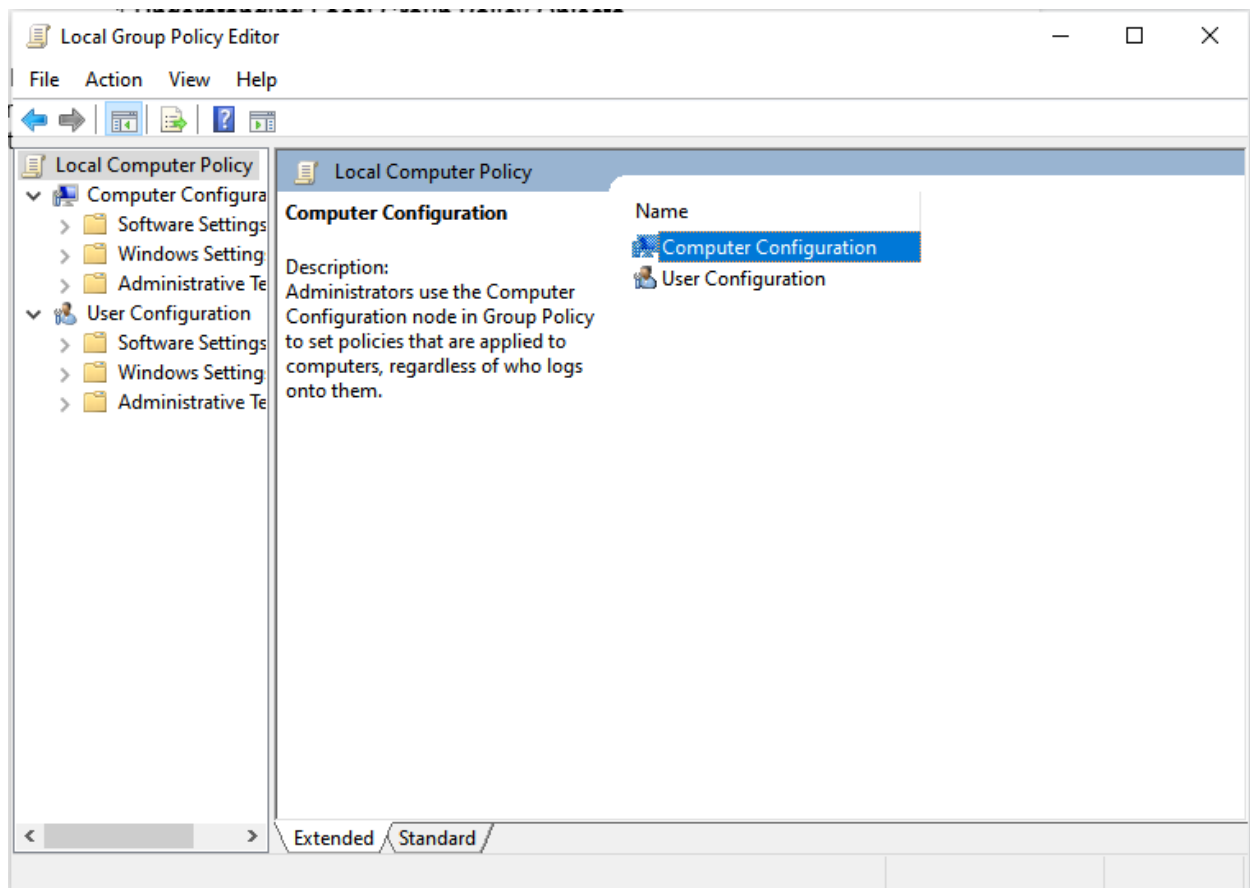


## Lab Session-3

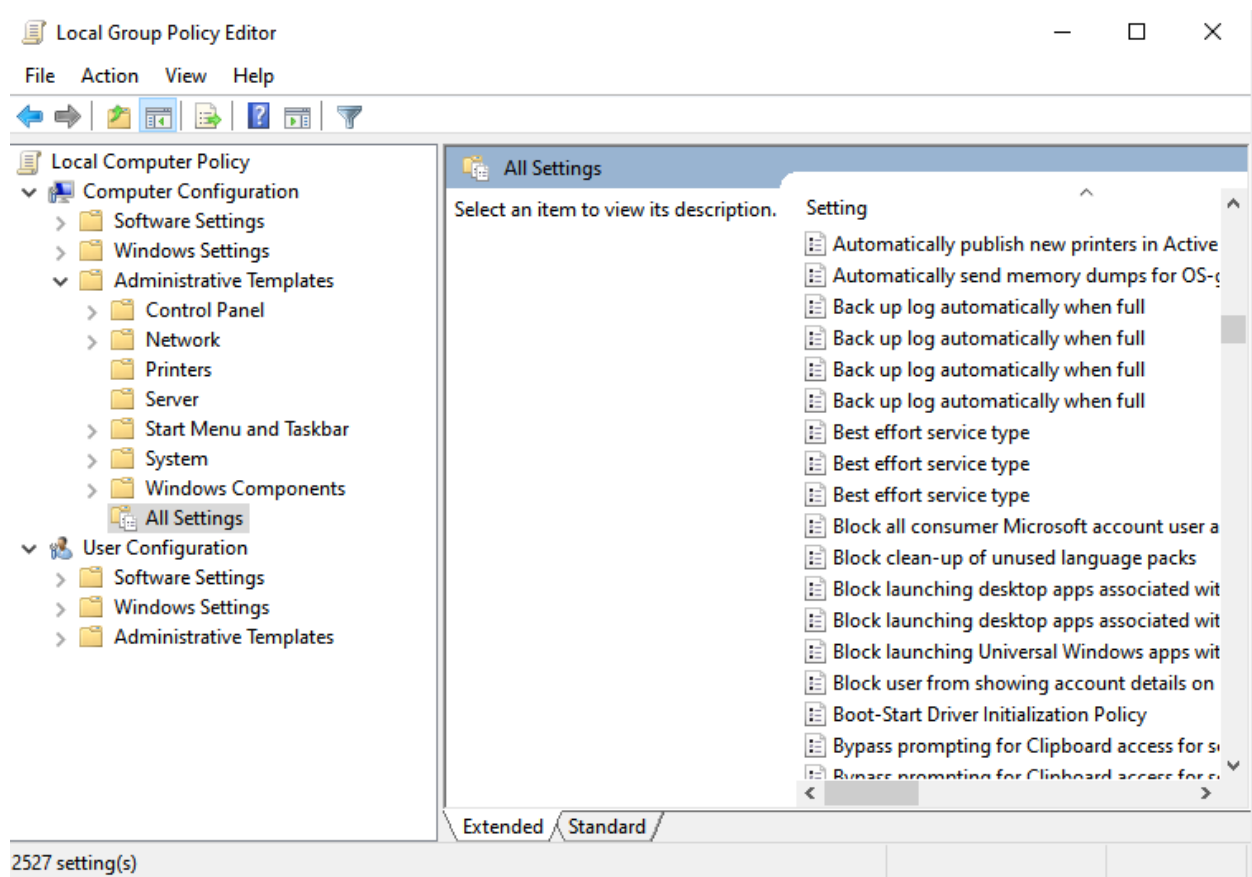
### 1. Understanding Local Group Policy Objects

A local Group Policy Object refers to the collection of group policy settings that only apply to the local computer and to the users who log on to that computer. Local GPOs are used when policy settings need to apply to a single Windows computer or user.



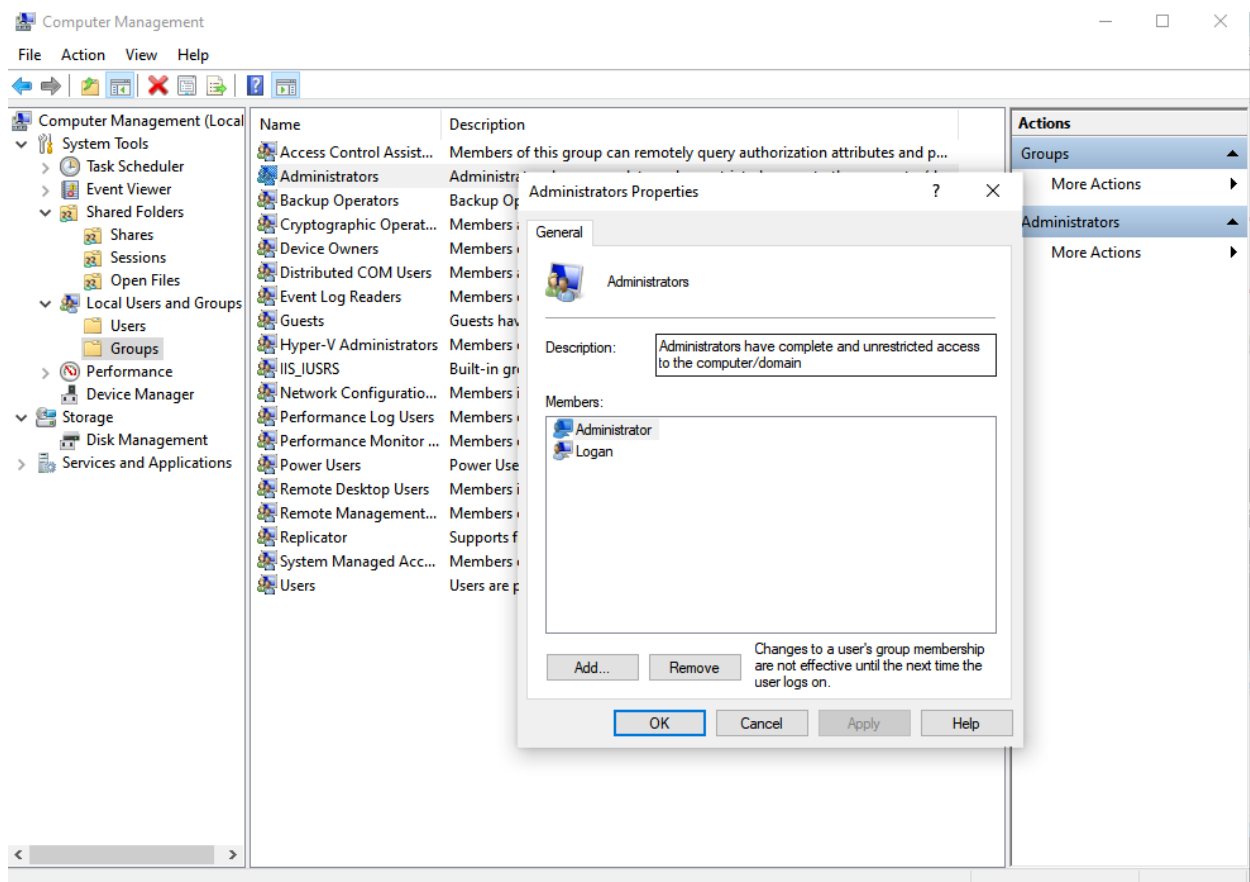
## 2. Understanding Domain Group Policy Objects

AD Group Policies are critical pieces of instructions in an AD environment that an IT administrator can configure. AD group policies will determine the behavior and privileges for users and computers. Group Policies are primarily a security solution for the AD network. Administrators can configure these settings and then implement sets of these settings on sites, domains, or OUs containing users and computers.



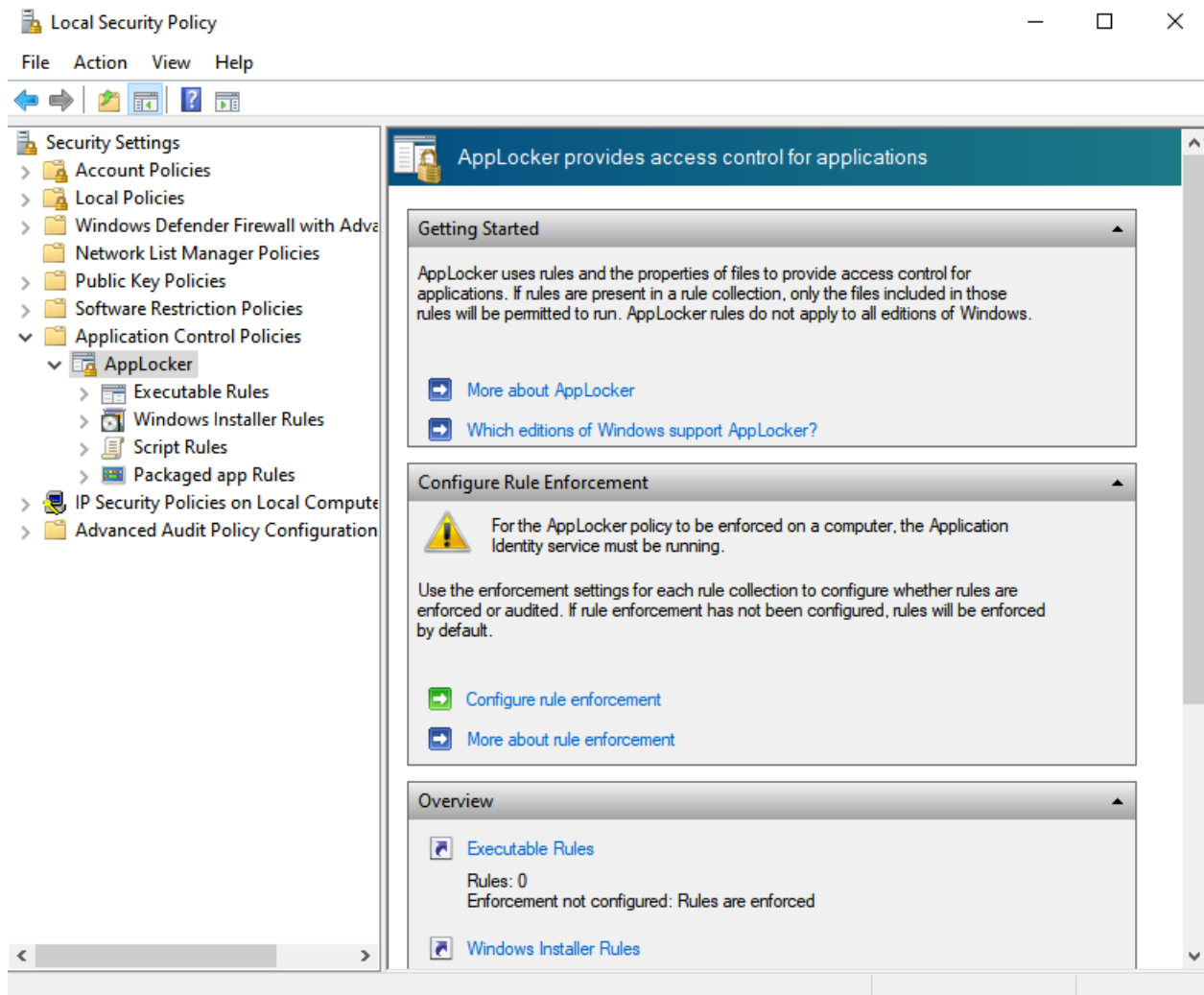
### 3.Administrative Users

Administrative users have full or restricted access to the Security Groups application and to the Users application. Administrative users are responsible for implementing and maintaining security services, such as adding users, building profiles, or managing general site administration.



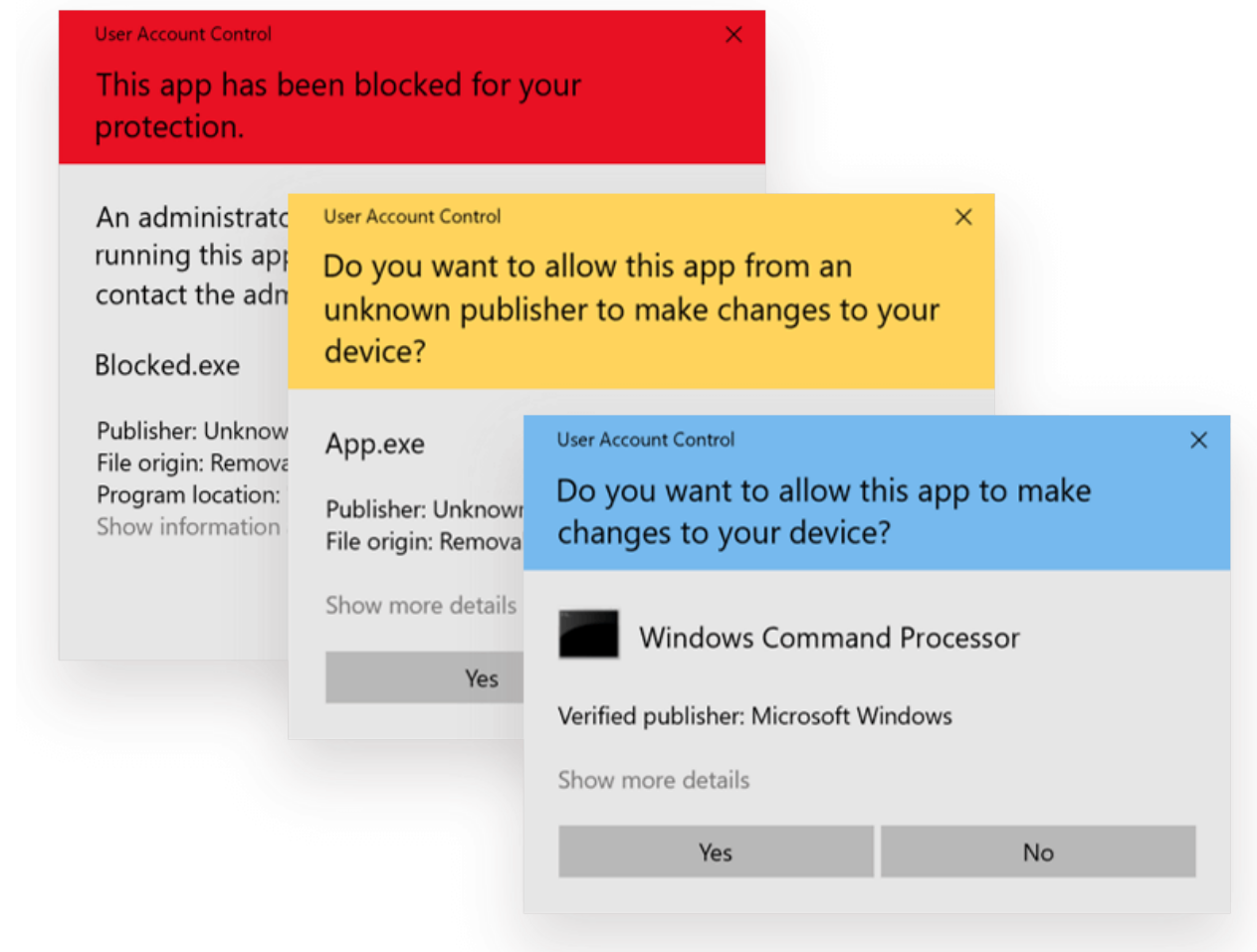
## 4.AppLocker

AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.



## **5.User Account Control**

User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware. User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

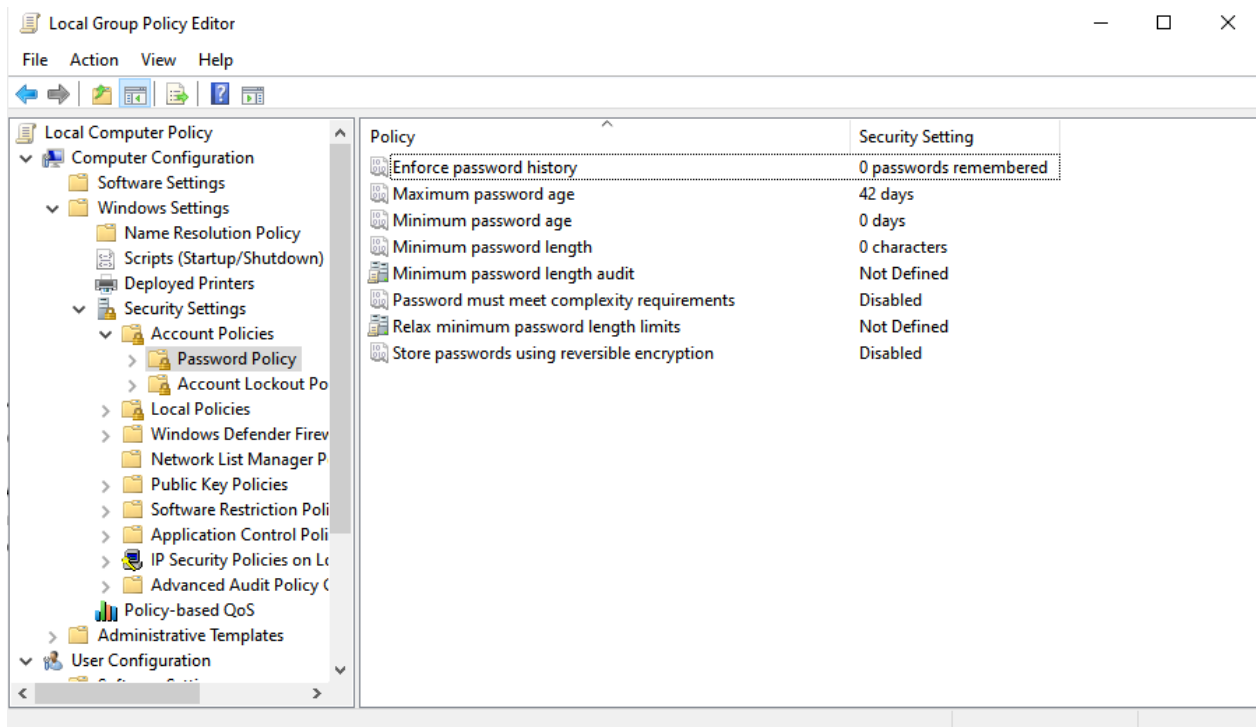


## 6.Checking Recommended GPO settings

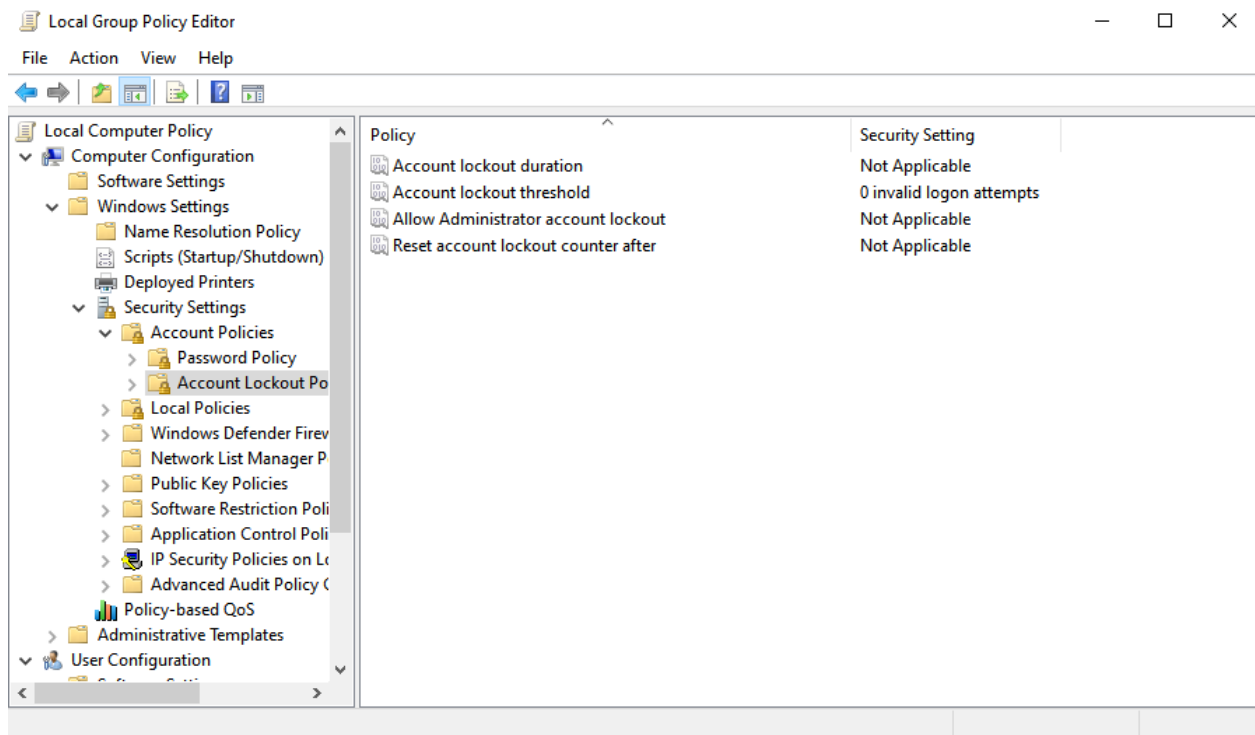
You can generate HTML-based and XML-based reports for reviewing settings within any version of a Group Policy object (GPO).

A user account with the Reviewer, Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

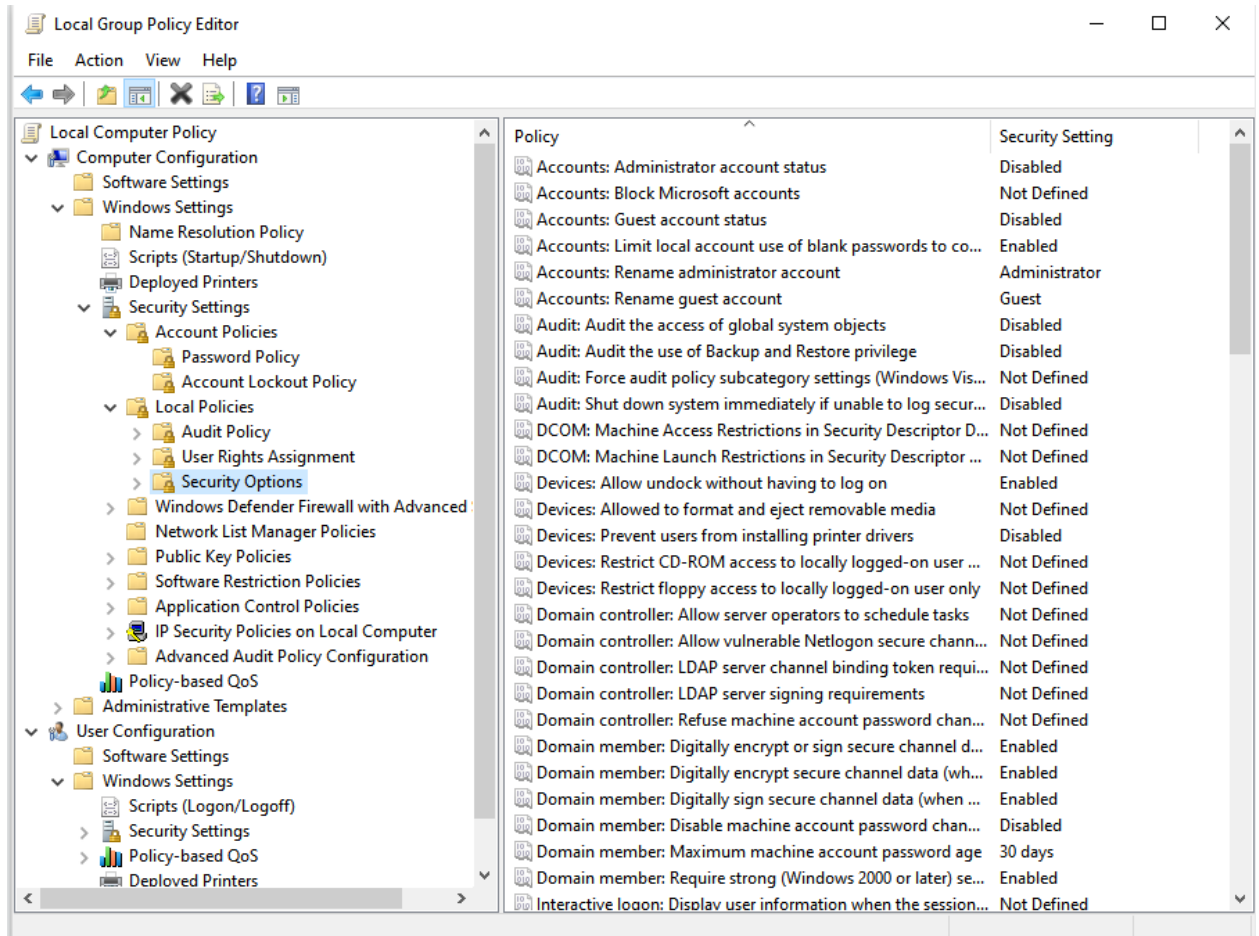
### **a. Password Policy**



## b. Account Lockout Policy



### c. Security options





#### d. Internet Explorer Security.

