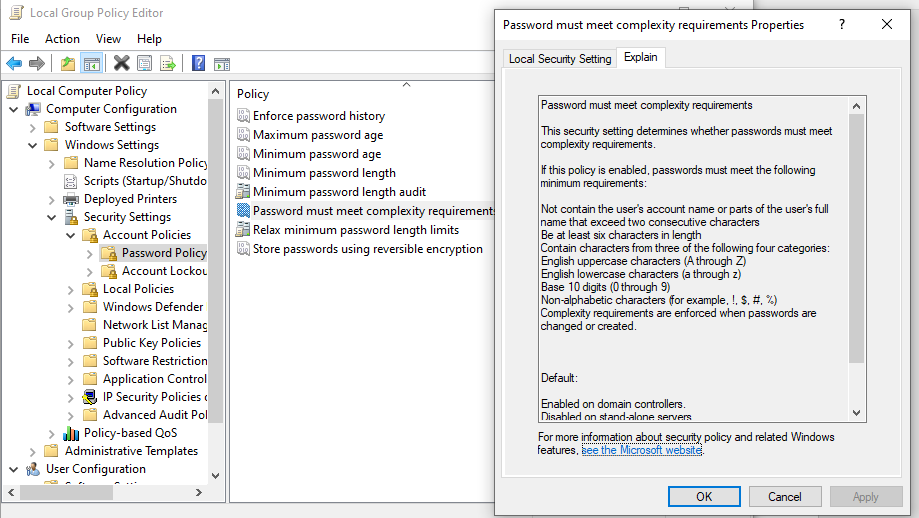
In Windows systems, group policies (GPOs) are configurations and settings that are used to manage and regulate user and machine settings. The paper contains five typical Group Policies that can be used in a Windows domain context.

**Enforce the rules for password complexity**

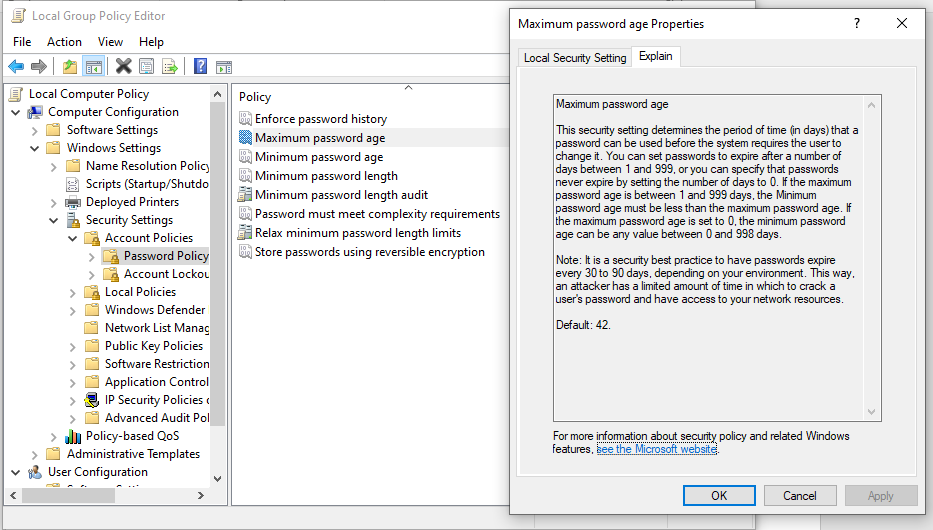
The complexity requirements for passwords are determined by this security parameter. Passwords must adhere to the following minimum requirements if this policy is enabled:

1. Do not have more than two consecutive characters from the user's complete name or account name.
2. Have a minimum of six characters.
3. Characters that fall within three of the following four categories: (A through Z) Uppercase letters in English, Lowercase letters in English (a through z). Base 10 digits, from 0 to 9. Non-alphabetic characters, such as!, $, #, and %



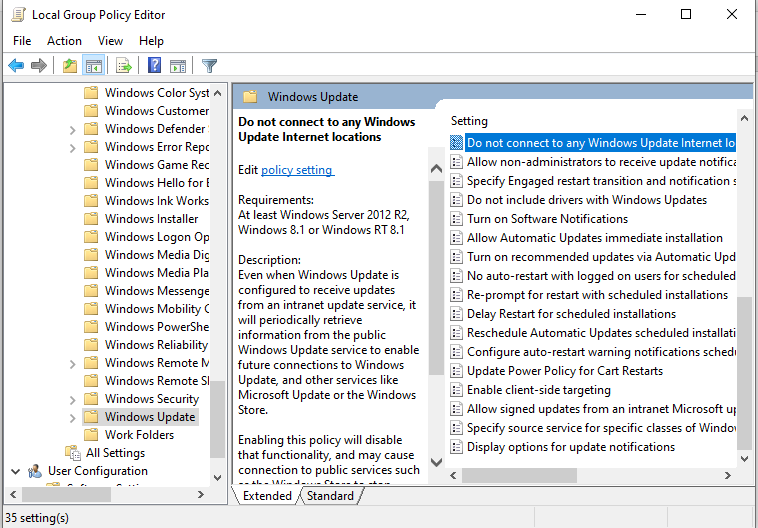
**Set a password's minimum and maximum age**

The security feature enables to set the period of time that a password can be used before the system requests the user to change the password. The feature is essential in a way that it provides a limited amount of time to crack a user’s password and gain access to a user’s network resources.



**Windows Update Policy**

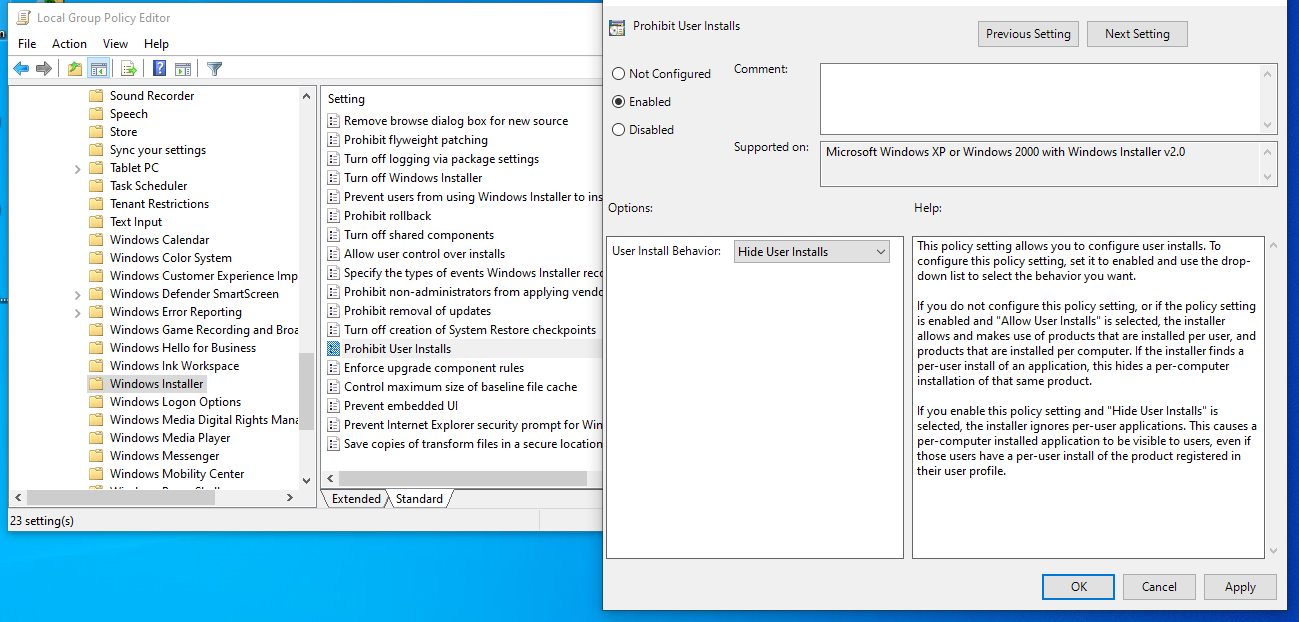
The policy helps domain-joined machines handle Windows updates and control the options and time frames for updating. There are various sub-policies under Windows update. An individual has the permission to enable the permission which will meet a person’s specified needs.



**Restriction for Installing Software**

The policy helps in managing and deploying software installations on computers connected to a network. Additionally, it controls when and what software is installed. Granting users the ability to install software can result in the installation of unwanted applications that pose a risk to your system's integrity (Hinckley, 2020). As a consequence, system administrators often find themselves engaged in periodic system maintenance and cleanup efforts. To ensure a more secure computing environment, it is advisable to restrict software installations using Group Policy:

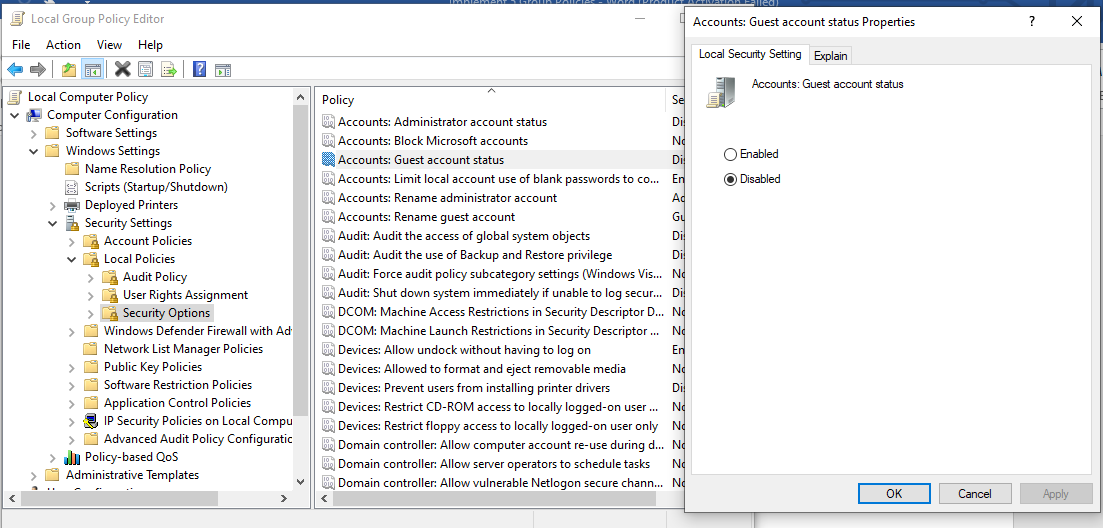
1. Launch the Group Policy Management Editor for a custom GPO.
2. Navigate to "Computer Configuration" -> "Administrative Templates" -> "Windows Components" -> "Windows Installer."
3. In the right-hand pane, double-click the "Prohibit User Installs" policy.
4. Select the "Enabled" option to activate the policy.
5. Confirm the changes by clicking "Apply" and then "OK."



**Disabling the Guest Account**

Enabling the Guest Account provides users with unrestricted access to sensitive data on a Windows computer without requiring a password (Murphy, 2017). Enabling this account creates a situation where anyone could potentially misuse and exploit access to your systems. It is advisable to verify that this is the case within the IT environment because if this account is enabled in an individual’s domain, deactivating it will help prevent unauthorized access:

1. Open the Group Policy Management Editor for a custom GPO.
2. Navigate to "Computer Configuration" -> "Windows Settings" -> "Security Settings" -> "Local Policies" -> "Security Options."
3. In the right-hand pane, double-click the "Accounts: Guest Account Status" policy.
4. Check the "Define this policy setting" box and select "Disabled."
5. Confirm the changes by clicking "Apply" and then "OK."



**Creating Group Policy Objects**

Open Group Policy Management Console (GPMC) (Brown, 2022)

1. Create a New GPO
2. In the GPMC window, expand the forest and domain trees to locate your domain.
3. Right-click on the "Group Policy Objects" container under your domain and select "New."
4. Give your GPO a meaningful name, such as "Sales."

Linking the Group Policy Objects to the Sales OU

1. In the GPMC window, navigate to the "Sales" OU (or the OU where you want to link the GPO).
2. Right-click on the "Sales" OU and select "Edit."
3. In the Group Policy Management Editor, navigate to "Computer Configuration" or "User Configuration," subject to the settings the user wants to apply (Brown, 2022).
4. Configure the settings as per user requirements within the GPO.

**Delegating Administrator Control to a User (Jon Packer)**

In the GPMC window, right-click on the "Sales" OU (or the OU you linked the GPO to) and select "Delegate Control." In the Delegate Control Wizard click "Next" on the welcome screen. Click "Add..." to select the user an individual wants to delegate control to (Username). The next step is following the wizard to select a username from the Active Directory (Brown, 2022).

The next step is assigning the tasks. On the "Tasks to Delegate" screen, select "Create, delete, and manage user accounts" if a person needs the username (Jon Packer) to manage user accounts within the Sales OU. Other tasks can be selected based on the user requirements. Verifying that the GPO is linked to the Sales OU and that the username (Jon Packer) has the delegated control a user-specified. After finishing the setup process user (Jon Packer) will have the delegated control to manage user accounts or other specified tasks within the Sales OU, and the GPO created will apply the desired policies to computers or users within that OU (Brown, 2022).

**Conclusion**

The absence of Group Policy Settings can lead to a multitude of issues that you would prefer to avoid. This is particularly appropriate as individuals prepare their organizations to adapt to the evolving landscapes of remote work and cloud-based operations. Ensuring the proper configuration of Group Settings provides an opportunity to enhance both productivity and security. It is important to remember that these settings are valuable even if the need for a swift transition to remote work is not imminent. Taking the time to become familiar with these settings is crucial.

**References**

Brown, J. (2022). *12 Group Policy Best Practices: Settings and Tips for Admins | Varonis*. Www.varonis.com. <https://www.varonis.com/blog/group-policy-best-practices>

Hinckley, M. (2020, December 7). *7 Most Useful AD Group Policy Settings*. CBT Nuggets Blog. <https://www.cbtnuggets.com/blog/certifications/microsoft/7-most-useful-ad-group-policy-settings>

Murphy, D. (Ed.). (2017, December). *Top 10 Most Important Group Policy Settings for Preventing Security Breaches - Lepide Blog: A Guide to IT Security, Compliance and IT Operations*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. <https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/>