Step by step implementation of password policy settings

Setting up a good password policy for your organization can help prevent an attacker from playing the role of a legitimate user and thereby prevent data loss, sensitive information disclosure.

Review part I: Set up a secure password system

In this section we will provide you with step-by-step instructions on advanced security by implementing password settings on the computers in your organization.

1. Configure password policy settings in an Active Directory-based domain
2. Configure password policy settings on individual computers

Configure password policy settings in an Active Directory domain

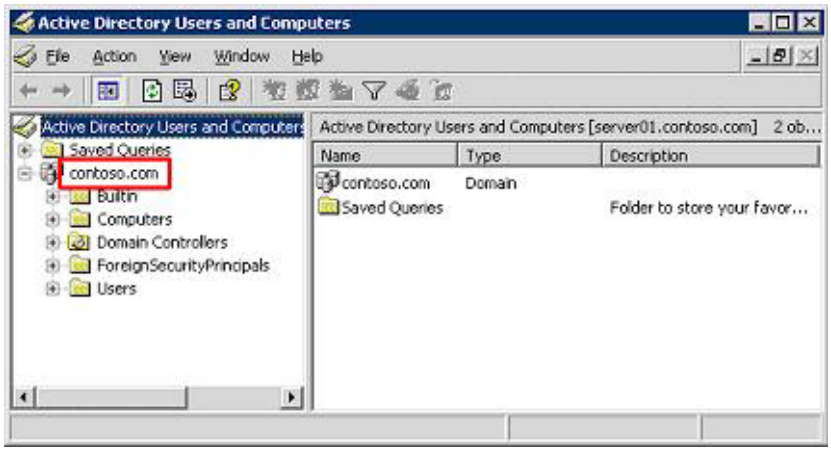
Request

• *Requirements* : You must be logged in as a member of the domain admin group.

• *Tools* : Active Directory Users and Computers

• To enforce password policies on the computer system of an Active Directory domain

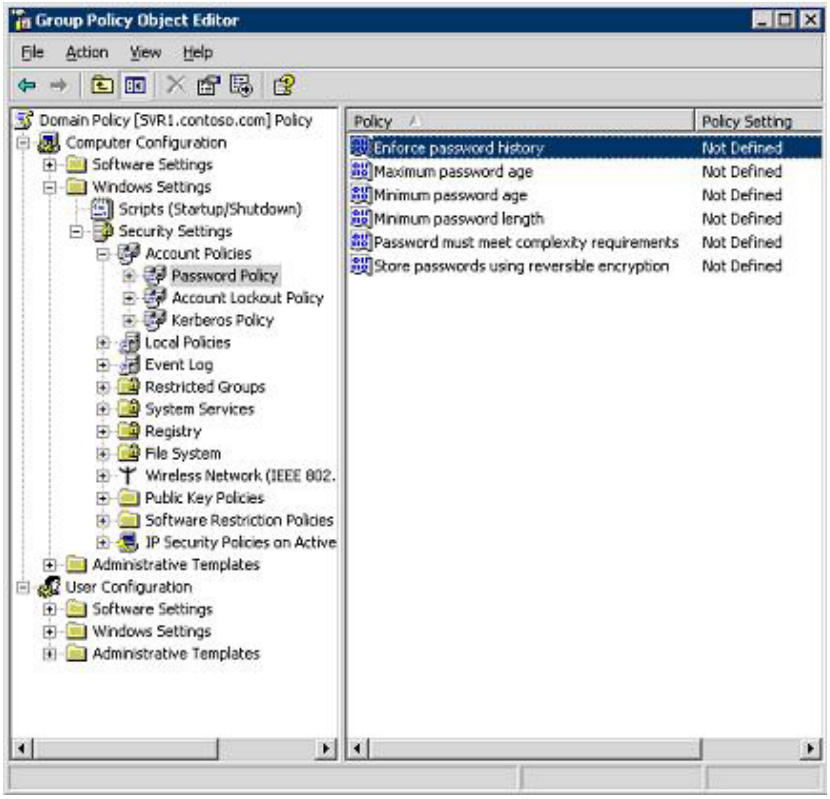
1. **Go to Start** > **Control Panel** , double-click **Administrative Tools,** and then double-click **Active Directory Users and Computers** .
2. Right-click on the domain root
3. Select **Properties** from the menu that appears:



Note : The image in this document is a test environment and information may change with the information displayed on your screen.

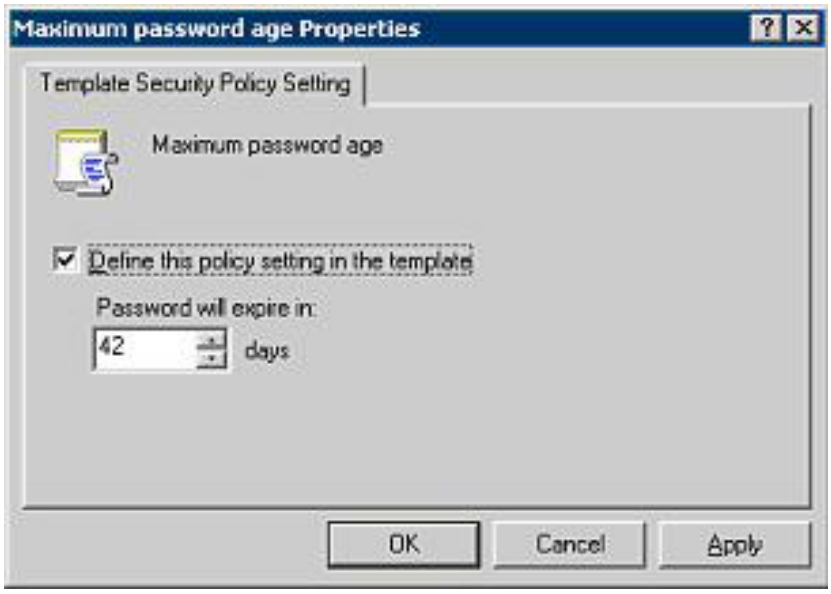
4. In the properties dialog box, select the **Group Policy** tab, and then click **New** to create a new group policy object in the domain root. Enter " *Domain Policy* " for the name of the new policy and then click **Close** .

   Note : Microsoft recommends that you create a new Group Policy object instead of editing the so-called **Default Domain Policy** because it is easier to recover important issues with security settings. . If new security settings cause problems, you can temporarily disable the new Group Policy object until you isolate those settings.
5. Right-click on the domain root, then click **Properties** .
6. In the properties dialog box, click the **Group Policy** tab, and then select **Domain Policy** .
7. Click **Up** to move the new GPO to the top of the list, then click **Edit** to open the **Group Policy Object Editor** for the GPO you created.
8. Under **Computer Configuration** , navigate to the Windows SettingsSecurity SettingsAccount PoliciesPassword Policy folder



9. In the details pane, double-click **Enforce password history** , select **Define this policy setting** , set the value of **Keep password history to 24** and then click **OK** .

10. In the details window, double-click **Maximum password age** , select **Define this policy setting** and set the value of **Password will expire in 42** , click **OK** then click **OK** to close the **Suggested Value Changes** window that appears.



11. In the details window, double-click **Minimum Password Age** , select **Define this policy setting** and set the value of **Password to be changed after** is **2** and then click **OK** .

12. In the details window, click Double **Minimum Password Length** , select **Define this policy setting** and set the value of the **Password to be at least 8** and then click **OK** .

13. In the details window, double-click **Password must meet complexity requirements** , select **Define this policy setting in the template** , select **Enabled** then click **OK** .

14. Close the **Group Policy Object Editor** , click **OK** to close the domain properties dialog box, and then exit **Active Directory Users and Computers** .

Check for new settings

Use the procedure below to check if the appropriate password policy settings have been accepted and valid in the GPO Domain Policy. Check their settings and operations to make sure that the correct password policies are applied to domain users.

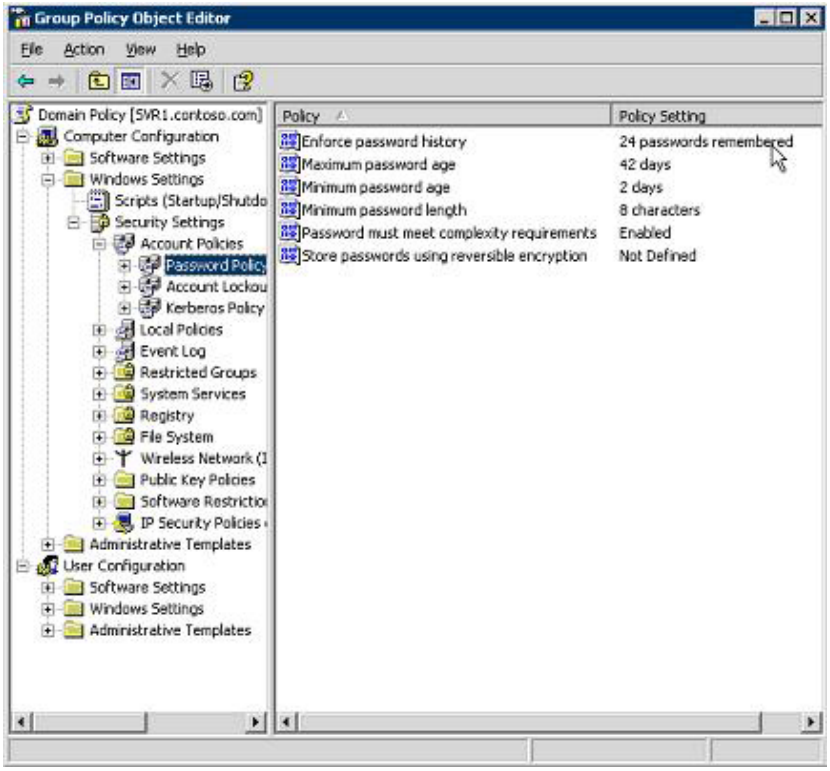
Request

• *Requirements* : You must be logged in as a member of the Domain Admins group

• *Tools* : Active Directory Users and Computers.

• To check password policy settings for an Active Directory domain

1. Open **Active Directory Users and Computers** , right-click your domain, then click **Properties** .
2. In the properties dialog box, click the **Group Policy** tab, select the **Domain Policy GPO,** and then click **Edit** to open the **Group Policy Object Editor** .
3. Under **Computer Configuration** , go to the Windows SettingsSecurity SettingsAccount PoliciesPassword Policy folder and check if your settings are correct with the settings shown here:



4. Close the **Group Policy Object Editor** , click **OK** to close the properties dialog for your domain, then exit **Active Directory Users and Computers** .
5. Checking to ensure that users cannot specify passwords shorter than 8 characters, unable to create complex passwords and cannot immediately change their new passwords.

Configure password policy settings on stand-alone computers

Request

• *Requirements* : You must be logged in as a member of the Administrators group.

• *Tool* : Local Security Policy.

• To implement password policy on non-Active Directory computer systems, proceed as follows:

1. **Go to Start** , click **Control Panel** , double-click **Administrative Tools** and then double-click **Local Security Policy** .
2. Navigate to the Account PoliciesPassword Policy folder.
3. In the details window, double-click **Enforce password history** , set the value of **Keep password history to 24** , and then click **OK** .
4. In the details window, double-click **Maximum password age** , set the value of **Password will expire in to 24** , and then click **OK** .
5. In the details window, double click on **Minimum Password Age** , set the value of **Password can be changed after 2** , then click **OK** .
6. In the details window, double click on **Minimum Password Length** , set the value of **Password to be at least 8** , then click **OK** .
7. In the details window, double-click the **Password must meet complexity requirements** , select **Enabled,** and then click **OK** .
8. Close **Local Security Policy** .

Check for new settings

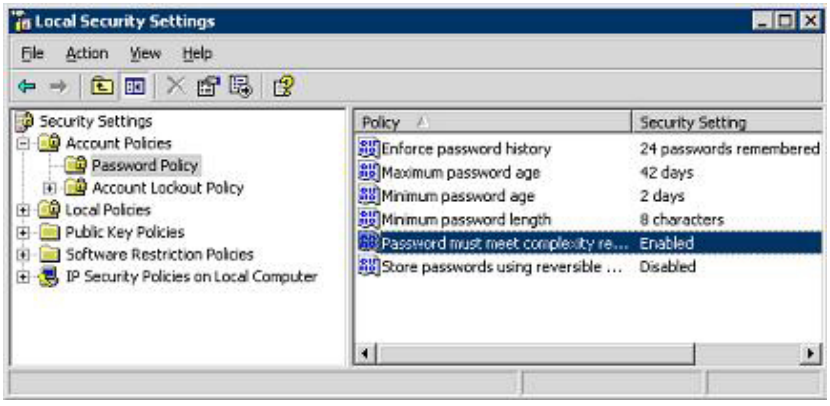
Request

• *Requirements* : You must be logged in as a member of the Administrators group.

• *Tool* : Local Security Policy.

• To check password policy settings for this computer system, follow these steps:

1. Open **Local Security Policy** , navigate to the Account PoliciesPassword Policy folder and check if your settings are correct for the settings shown here:



2. Close **Local Security Policy** .
3. Check to ensure that users cannot specify passwords that are shorter than 8 characters, cannot create non-complex passwords, and cannot change their new passwords immediately.

You finished reading the article "**Step by step implementation of password policy settings**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.