Managing Access Control Control in Windows Server

Scenario

In this activity, you will explore the use of different kinds of accounts for managing objects in Active Directory and the use of GPO to apply account policies.

Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 3.7 Given a scenario, implement identity and account management controls.

Lab

- DC1 VM

Task 1

Examine Administrator account properties

Implement some Microsoft best practices for securing administrative accounts and learn how not-such-best-practice can compromise organizational security. First, examine the properties of the current Administrator account.

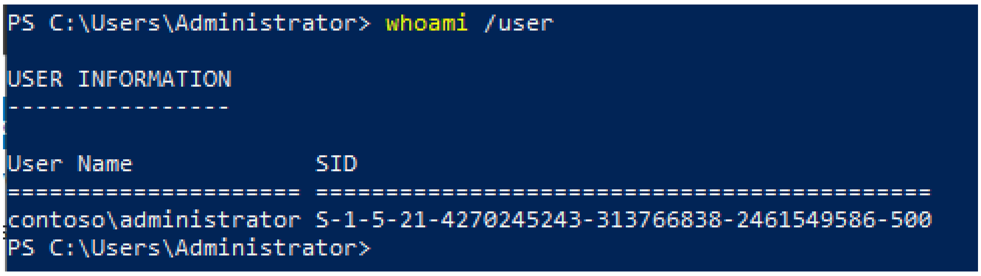
1. On the **DC1** VM, send **CTRL+ALT+DEL** and then sign in as **CONTOSO\Administrator** using **Pa$$w0rd** as the password.

2. Select the **Start** menu, right-click **Windows PowerShell**, and then select **Run as Administrator**.

NOTE: If prompted, confirm the UAC window selecting **Yes**.

3. Run the following command to display the Security ID (SID) and other information for the current user:

```
whoami /user
```



```
PS C:\Users\Administrator> whoami /user

USER INFORMATION
----------------

User Name             SID
===================== ============================================
contoso\administrator S-1-5-21-4270245243-313766838-2461549586-500
PS C:\Users\Administrator>
```

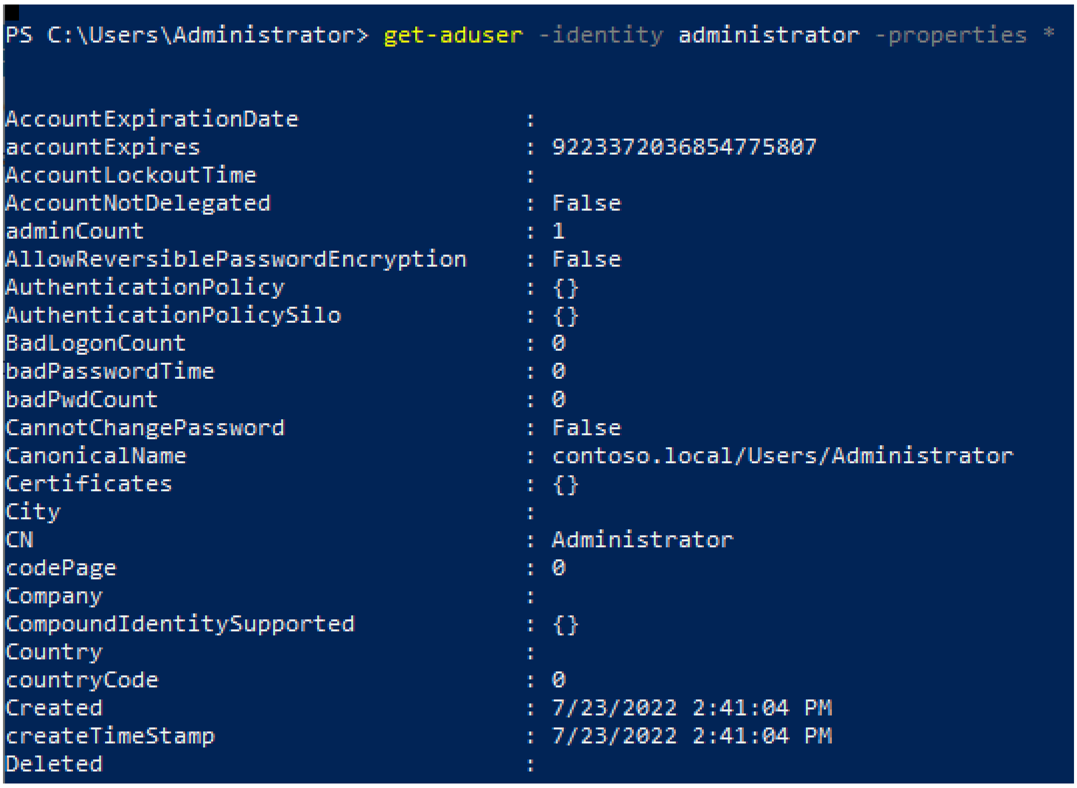
Figure 1.1 – The whoami command displaying the SID.

NOTE: User accounts are actually identified to the system by number, not by name. In Windows, this number is the Security Identifier (SID). In Linux, it is the User Identifier (UID).

TIP: You can use the **/all** switch with **whoami** to display additional group and privilege information.

4. Run the **get-aduser** cmdlet to display account information:

```
get-aduser -identity administrator -properties *
```



```
PS C:\Users\Administrator> get-aduser -identity administrator -properties *


AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
adminCount                           : 1
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : contoso.local/Users/Administrator
Certificates                         : {}
City                                 :
CN                                   : Administrator
codePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 7/23/2022 2:41:04 PM
createTimeStamp                      : 7/23/2022 2:41:04 PM
Deleted                              :
```

Figure 1.2 – The Get-ADUser cmdlet displaying the Administrator account information.

5. Minimize the **Administrator: Windows PowerShell** window.

Task 2

Manage user, group, and computer objects

Active Directory stores and manages objects that represent common entities, such as user accounts or computers. You will manage users, groups, and computer objects in this activity.

1. In **Server Manager**, from the **Tools** menu, open the **Active Directory Users and Computers** console.

2. Expand the **contoso.local** domain node.

3. Right-click the c**ontoso.local** domain node, select **New**, and then select **Organizational Unit**. Name the new OU **ITAdmins**.

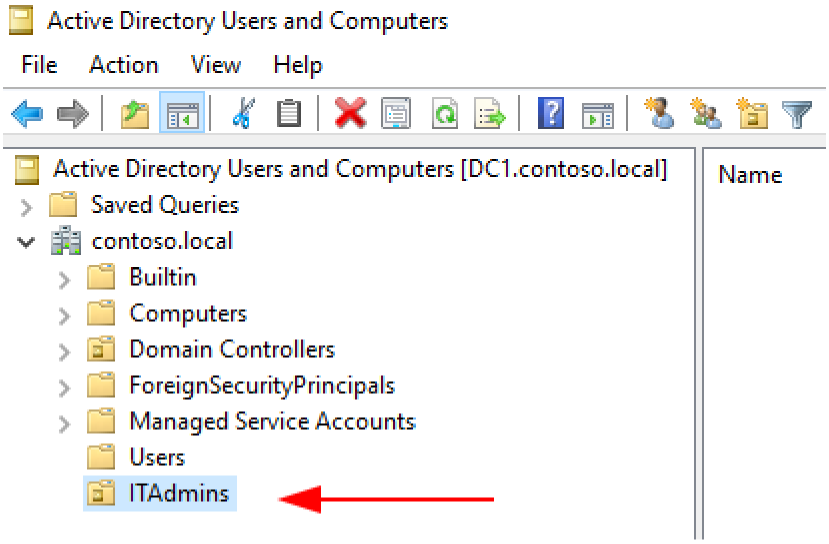
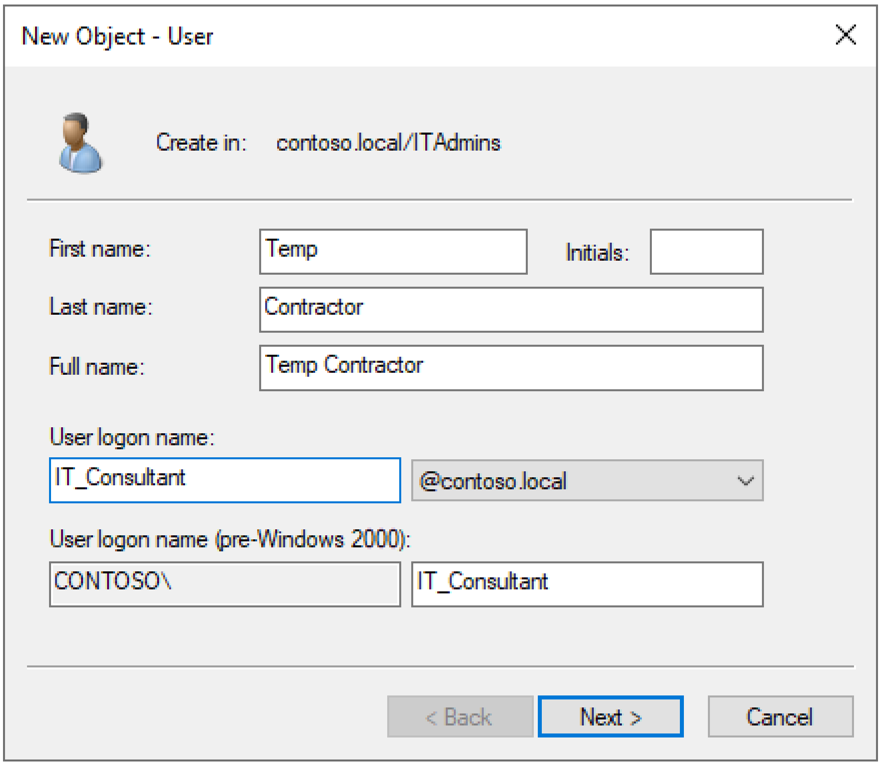


Figure 2.1 – ITAdmins Organizational Unit.

NOTE: Microsoft differentiates between the terms container and organizational units. An OU can have a Group Policy Object linked to it, which results in it being easier and more flexible to manage. Containers cannot have linked GPOs and are not typically used for day-to-day AD administration. Be sure to observe the difference in the icons between the Users container and the ITAdmins organizational unit.

4. Right-click the **ITAdmins** OU, select **New**, and select **User**. Create a new user named **IT_Consultant**.

- First name: Temp
- Last name: Contractor
- User login name: IT_Consultant
- Password: Pa$$w0rd



New Object - User

Create in: contoso.local/ITAdmins

First name: Temp

Initials:

Last name: Contractor

Full name: Temp Contractor

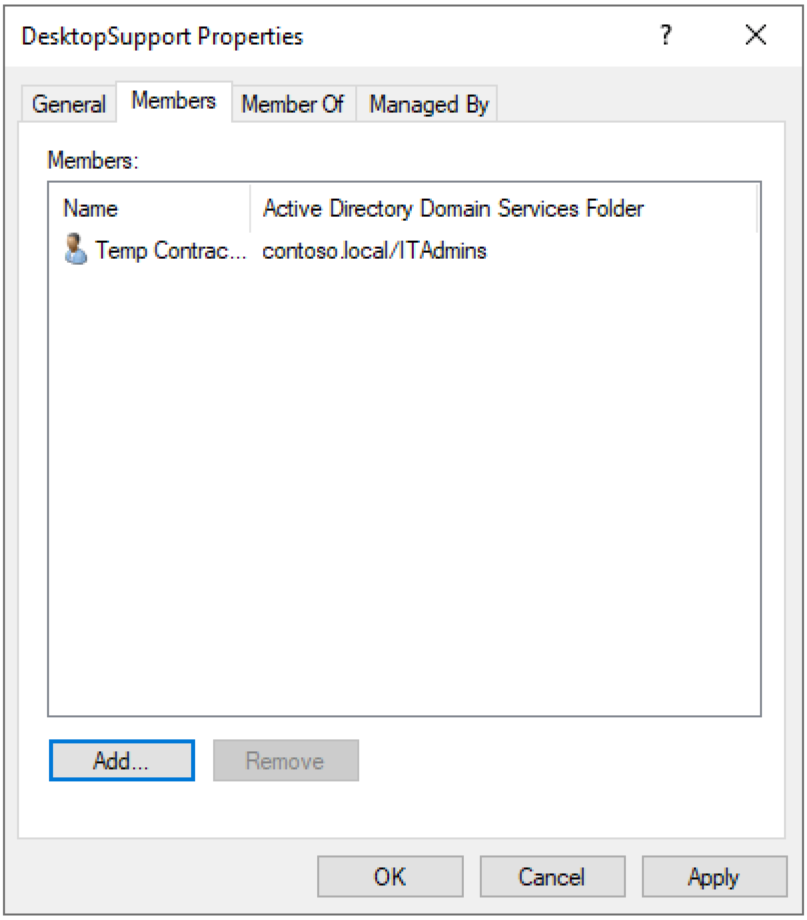
User logon name: IT_Consultant @contoso.local

User logon name (pre-Windows 2000): CONTOSO\ IT_Consultant

Figure 2.2 – New Object - User IT_Consultant.

5. Create a Global Security group within the **ITAdmins** OU and name it **DesktopSupport**.

6. Add the **IT_Consultant** account to the **DesktopSupport** group.



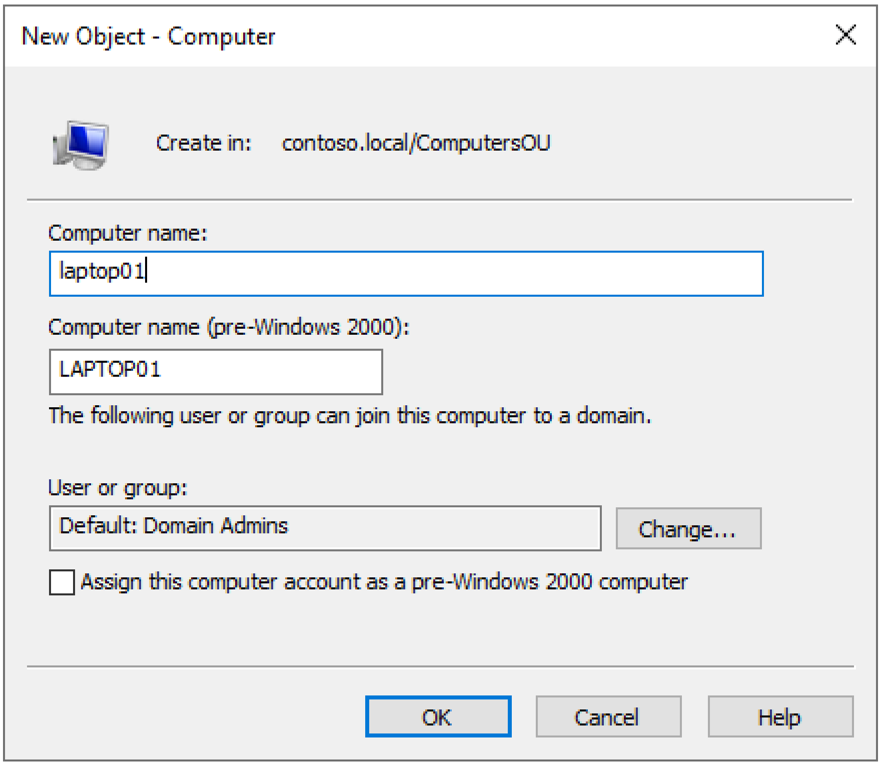
DesktopSupport Properties

Members:

Name	Active Directory Domain Services Folder
Temp Contrac...	contoso.local/ITAdmins

Figure 2.3 – DesktopSupport Group showing Temp Contractor user as a member.

7. From the **contoso.local** domain object, browse to the **ComputersOU** Organizational Unit, right-click it, select **New** and then create a new computer account named **laptop01**.



New Object - Computer

Create in: contoso.local/ComputersOU

Computer name: laptop01

Computer name (pre-Windows 2000): LAPTOP01

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins

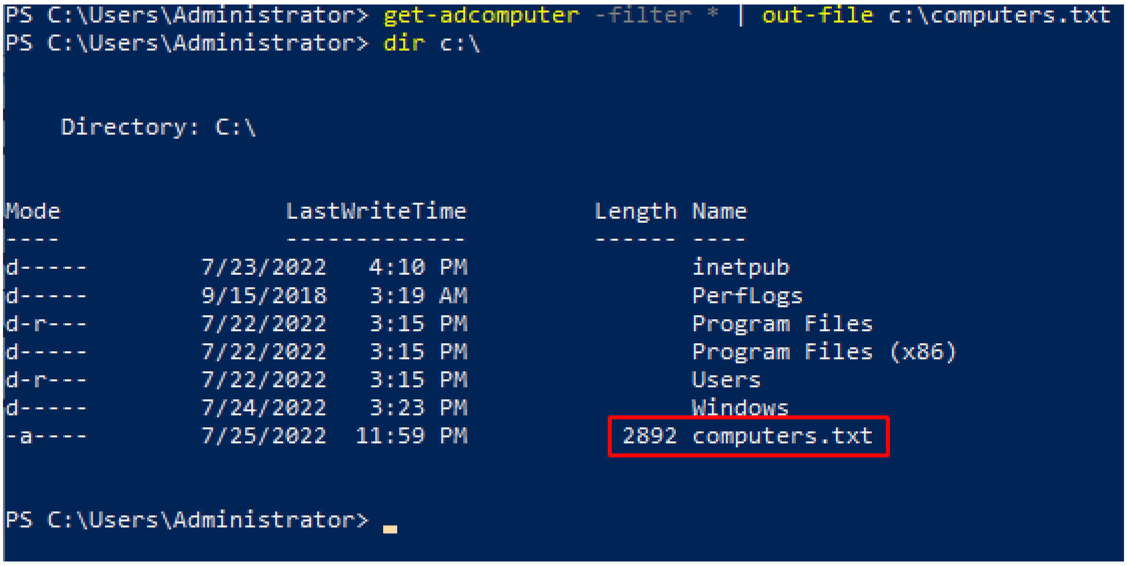
□ Assign this computer account as a pre-Windows 2000 computer

Figure 2.4 – New Object - Computer laptop01.

8. Run the following PowerShell cmdlet to generate a report of all computer objects in the domain.

```
get-adcomputer -filter * | out-file c:\computers.txt
```

9. Confirm that the **C:\computers.txt** file exists.



```
PS C:\Users\Administrator> get-adcomputer -filter * | out-file c:\computers.txt
PS C:\Users\Administrator> dir c:\


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         7/23/2022   4:10 PM                inetpub
d-----         9/15/2018   3:19 AM                PerfLogs
d-r---         7/22/2022   3:15 PM                Program Files
d-----         7/22/2022   3:15 PM                Program Files (x86)
d-r---         7/22/2022   3:15 PM                Users
d-----         7/24/2022   3:23 PM                Windows
-a----         7/25/2022  11:59 PM           2892 computers.txt


PS C:\Users\Administrator>
```

Figure 2.5 – The computer.txt file.

NOTE: You have created several types of Active Directory objects: users, groups, and computer accounts. You have also stored these objects in the appropriate Organizational Units so that Group Policy Object configurations can be easily applied to the correct OUs and impact the correct users and computers.

10. Minimize the **Administrator: Windows PowerShell** window.

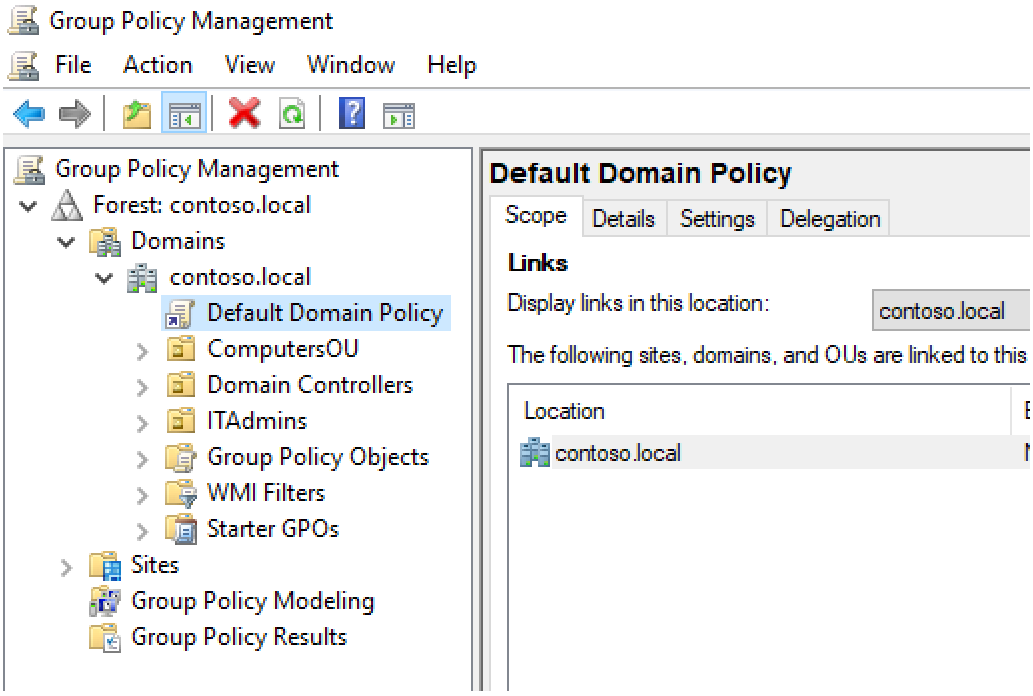
Task 3

Modify an existing GPO to match password requirements

Group Policy is a powerful tool enabling custom user and computer settings to be deployed to objects across Active Directory. Use the Group Policy Management console to examine the contoso.local Admin Policy.

1. In **Server Manager**, select **Tools** > **Group Policy Management**.

2. In the Group Policy Management console, expand **Forest** > **Domains** > **contoso.local** and select the **Default Domain Policy**.



Default Domain Policy

Links

Display links in this location: contoso.local

The following sites, domains, and OUs are linked to this

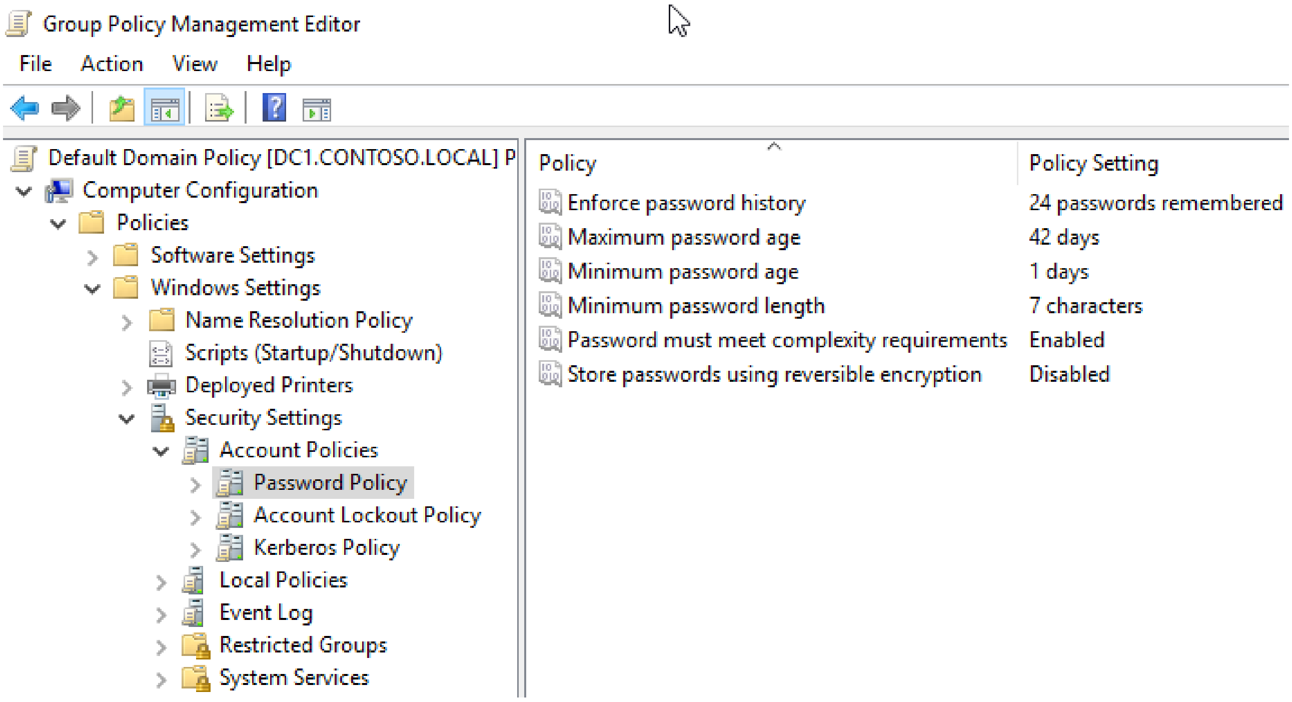
Location
contoso.local

Figure 3.1 – Group Policy Management console.

NOTE: The Default Domain Policy defines a single password policy for all members of the entire domain. Microsoft recommends that password management is the only use of the Default Domain Policy.

3. Right-click the **Default Domain Policy**, and then select **Edit**.

4. Browse to the **Password Policy** node by following this path: C**omputer Configuration** > **Policies** > **Windows Setting** > **Security Settings** > **Account Policies** > **Password Policy**.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Figure 3.2 – The Password Policy.

5. You have reviewed your company's written security policy regarding passwords. You must now configure the **Default Domain Policy** to match the following requirements. Double-click each Policy value to edit the settings.

Setting	Value	Explanation
Minimum Password Length	14 characters	All passwords must contain at least 14 characters.
Complexity Requirements	Enabled	Passwords must contain at least three of the following four characteristics: uppercase, lowercase, letters, numbers.
Maximum Password Age	90 days	Passwords must be changed every 90 days
Minimum Password Age	1 day	Passwords can only be changed once daily
Enforce Password History	20	Unique passwords that must be used before an old password may be repeated.
Enforce Reversible Encryption	Disabled	Makes it possible to decrypt passwords (not recommended)

Table 3.1 – Contoso's Password Security policies.

6. In the Administrator: Windows PowerShell window, run the following command to produce a report of the password policy settings to update configuration documentation:

```
gpresult /H C:\passwords-gpresults.html
```

7. Confirm that the **C:\passwords-gpresults.html** file exists.

NOTE: The Default Domain Policy (DDP) applies to ALL domain members, offering no flexibility to have different password policies for different kinds of users (stricter for high-privilege administrators but looser for non-privileged standard users, for instance). Fine grained password policies provide flexibility by enforcing different password requirements for specific users and groups. You will work with fine grained password policies in a later activity.