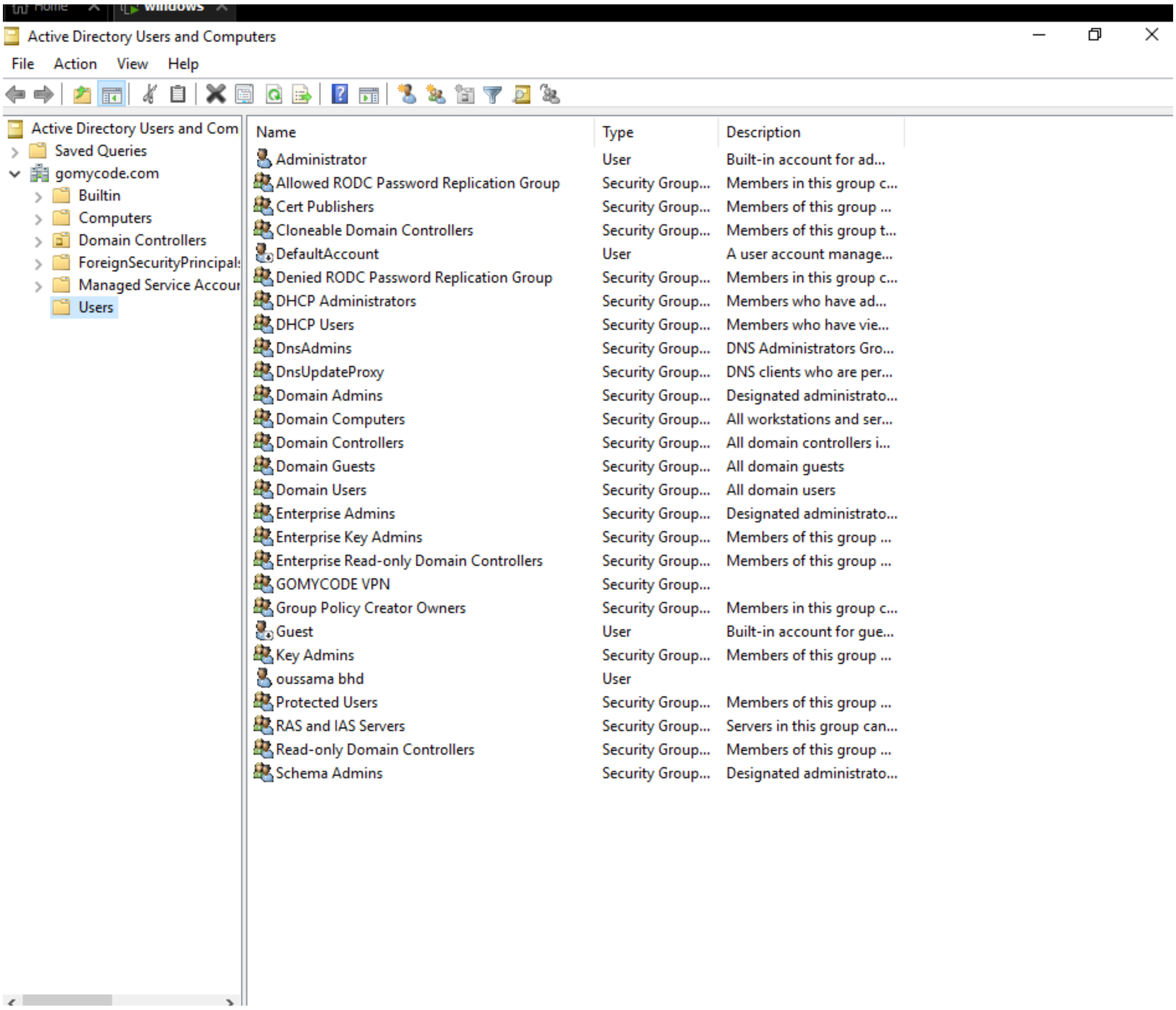
Checkpoint active defence

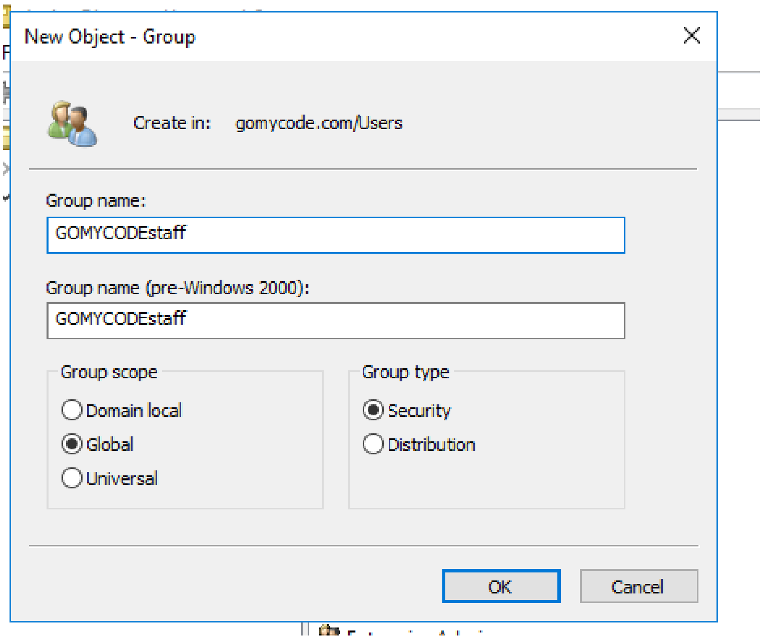
- first login to the windows server on the server manager goes to :

tools → Active Directory Users and Computers



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replication Group	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
DefaultAccount	User	A user account manage...
Denied RODC Password Replication Group	Security Group...	Members in this group c...
DHCP Administrators	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Key Admins	Security Group...	Members of this group ...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
GOMYCODE VPN	Security Group...	
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
oussama bhd	User	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...

- Right click on the user folder and choose the new group : https://i.imgur.com/hBBrhUc.png
- Create a group named GOMYCODEstaff: https://i.imgur.com/qzdFvgZ.png


New Object - Group

Create in: gomycode.com/Users

Group name:
GOMYCODEstaff

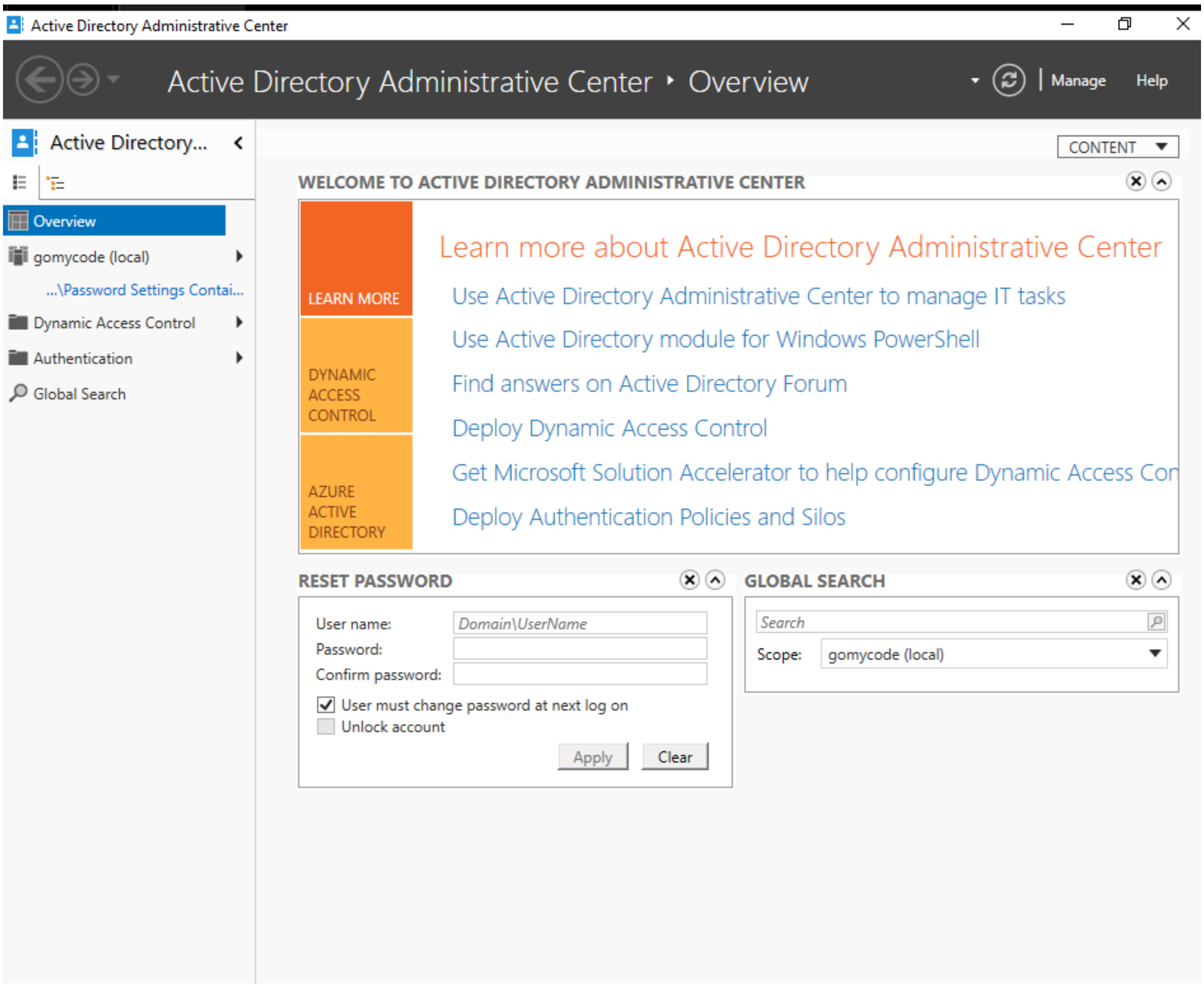
Group name (pre-Windows 2000):
GOMYCODEstaff

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

- now leave the User and Group Management and go to :

tools → Active Directory Administrative Center


Active Directory Administrative Center

Active Directory Administrative Center ‣ Overview

WELCOME TO ACTIVE DIRECTORY ADMINISTRATIVE CENTER

Learn more about Active Directory Administrative Center

Use Active Directory Administrative Center to manage IT tasks

Use Active Directory module for Windows PowerShell

Find answers on Active Directory Forum

Deploy Dynamic Access Control

Get Microsoft Solution Accelerator to help configure Dynamic Access Cor

Deploy Authentication Policies and Silos

RESET PASSWORD

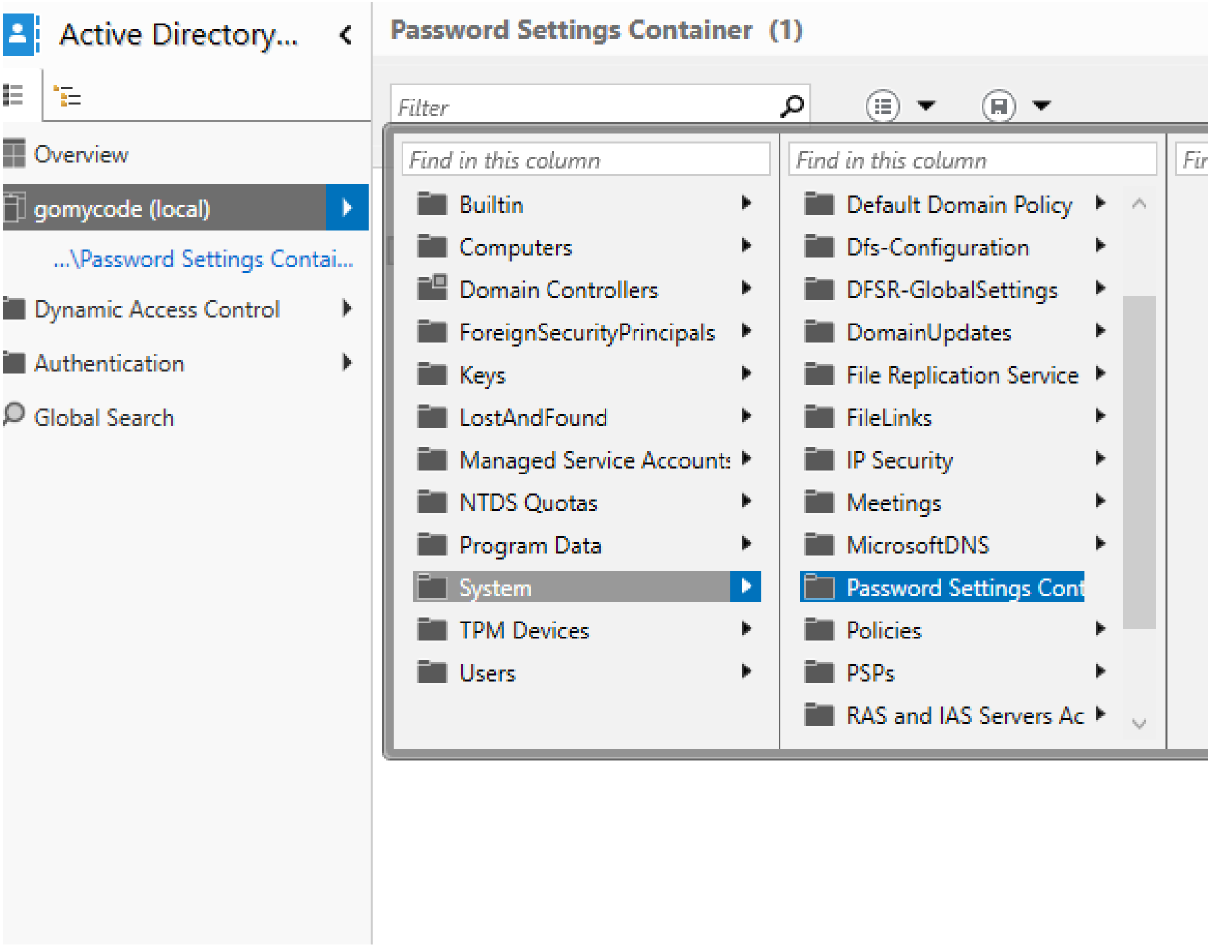
User name: Domain\UserName
Password:
Confirm password:
☑ User must change password at next log on
□ Unlock account

GLOBAL SEARCH

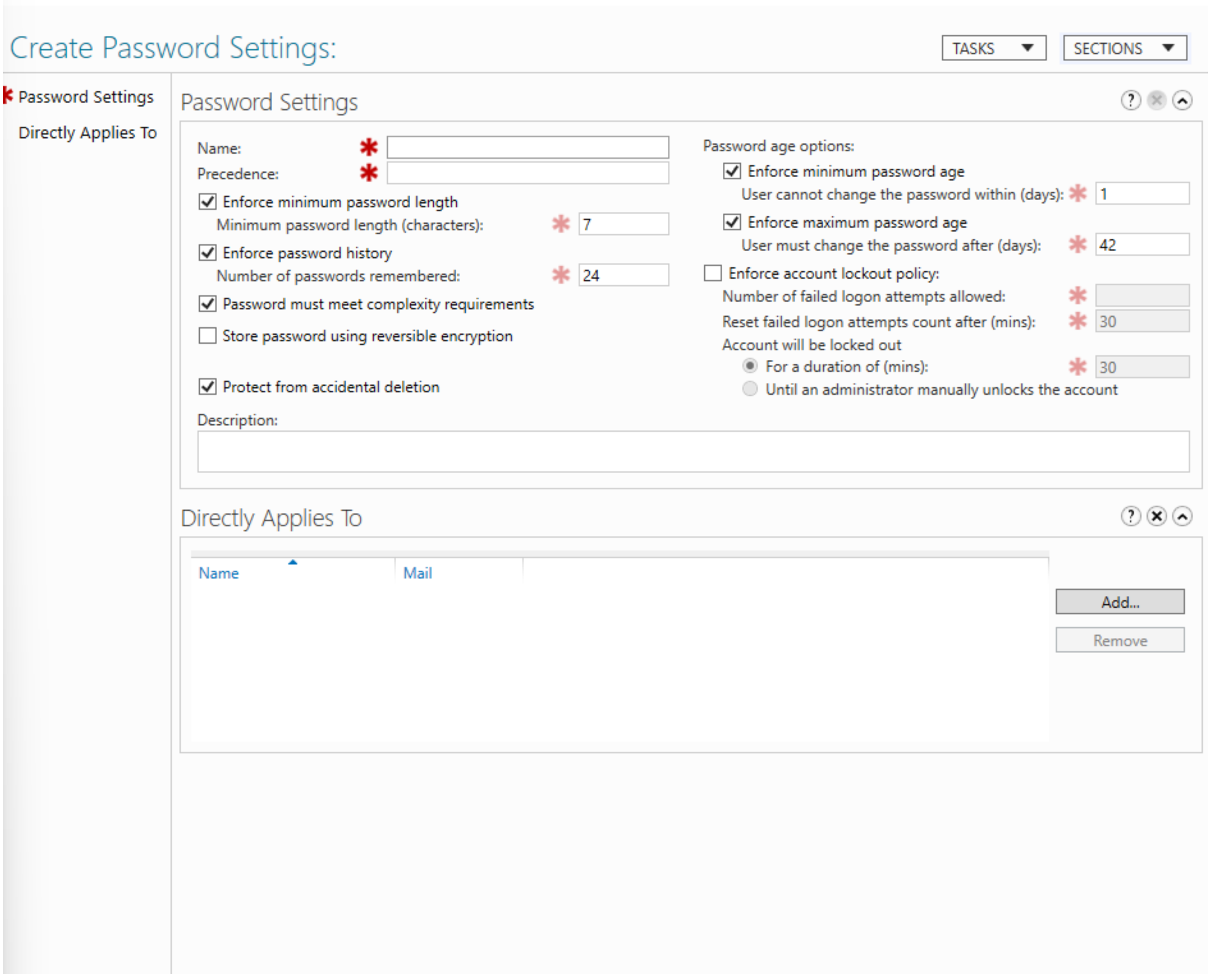
Scope: gomycode (local)

- On the left side choose:

gomycode (local) → system → Password settings



Now on the white space right click and choose new password settings :



Create Password Settings:

Password Settings

Name: *

Precedence: *

☑ Enforce minimum password length

Minimum password length (characters): * 7

☑ Enforce password history

Number of passwords remembered: * 24

☑ Password must meet complexity requirements

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:

☑ Enforce minimum password age

User cannot change the password within (days): * 1

☑ Enforce maximum password age

User must change the password after (days): * 42

☐ Enforce account lockout policy:

Number of failed logon attempts allowed: *

Reset failed logon attempts count after (mins): * 30

Account will be locked out

● For a duration of (mins): * 30

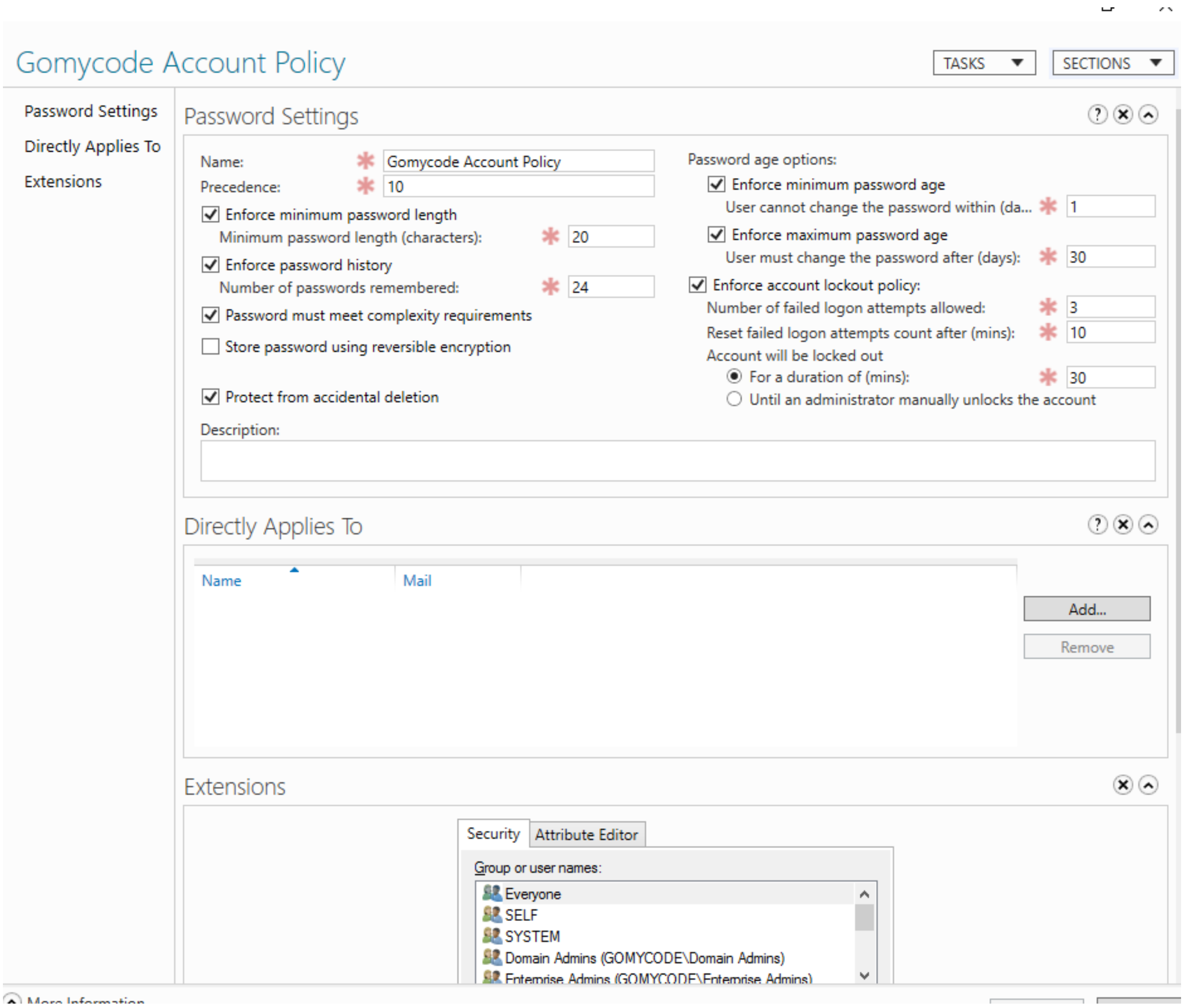
○ Until an administrator manually unlocks the account

Directly Applies To

Name	Mail

- **We want to configure the following policies:**
- All IT staff privileged accounts must contain a minimum of *20 characters* and be *complex*.
- Passwords must be changed every *30 days*. Passwords may not be changed more than *once per day* and the *24* most recent passwords cannot be repeated.
- IT staff-privileged accounts are subject to an *account lockout policy*, with a maximum of *three* failed login attempts allowed. Accounts will be locked out for a duration of *20 minutes*. Reset failed attempts after 10 minutes.
- Follow the following screen-shot: https://i.imgur.com/6qJJQzN.png
- click on **add**

- type **GOMYCODEstaff** in the enter the object names to select :



Gomycode Account Policy

Password Settings

Name: Gomycode Account Policy

Precedence: 10

☑ Enforce minimum password length

Minimum password length (characters): 20

☑ Enforce password history

Number of passwords remembered: 24

☑ Password must meet complexity requirements

☐ Store password using reversible encryption

☑ Protect from accidental deletion

Description:

Password age options:

☑ Enforce minimum password age

User cannot change the password within (da... 1

☑ Enforce maximum password age

User must change the password after (days): 30

☑ Enforce account lockout policy:

Number of failed logon attempts allowed: 3

Reset failed logon attempts count after (mins): 10

Account will be locked out

● For a duration of (mins): 30

○ Until an administrator manually unlocks the account

Directly Applies To

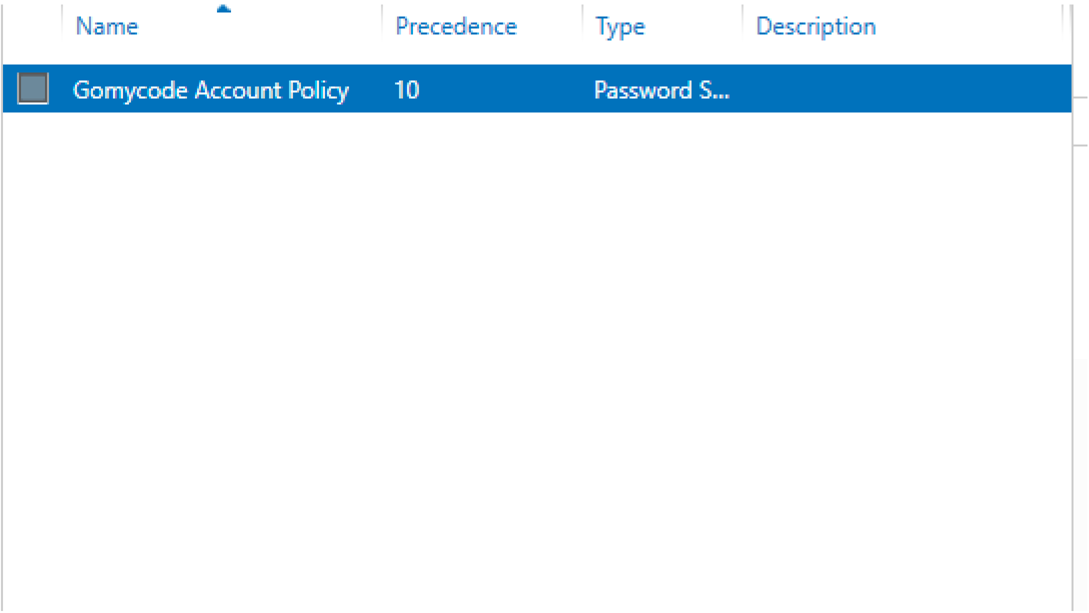
Name	Mail

Extensions

Group or user names:

Everyone
SELF
SYSTEM
Domain Admins (GOMYCODE\Domain Admins)
Enterprise Admins (GOMYCODE\Enterprise Admins)

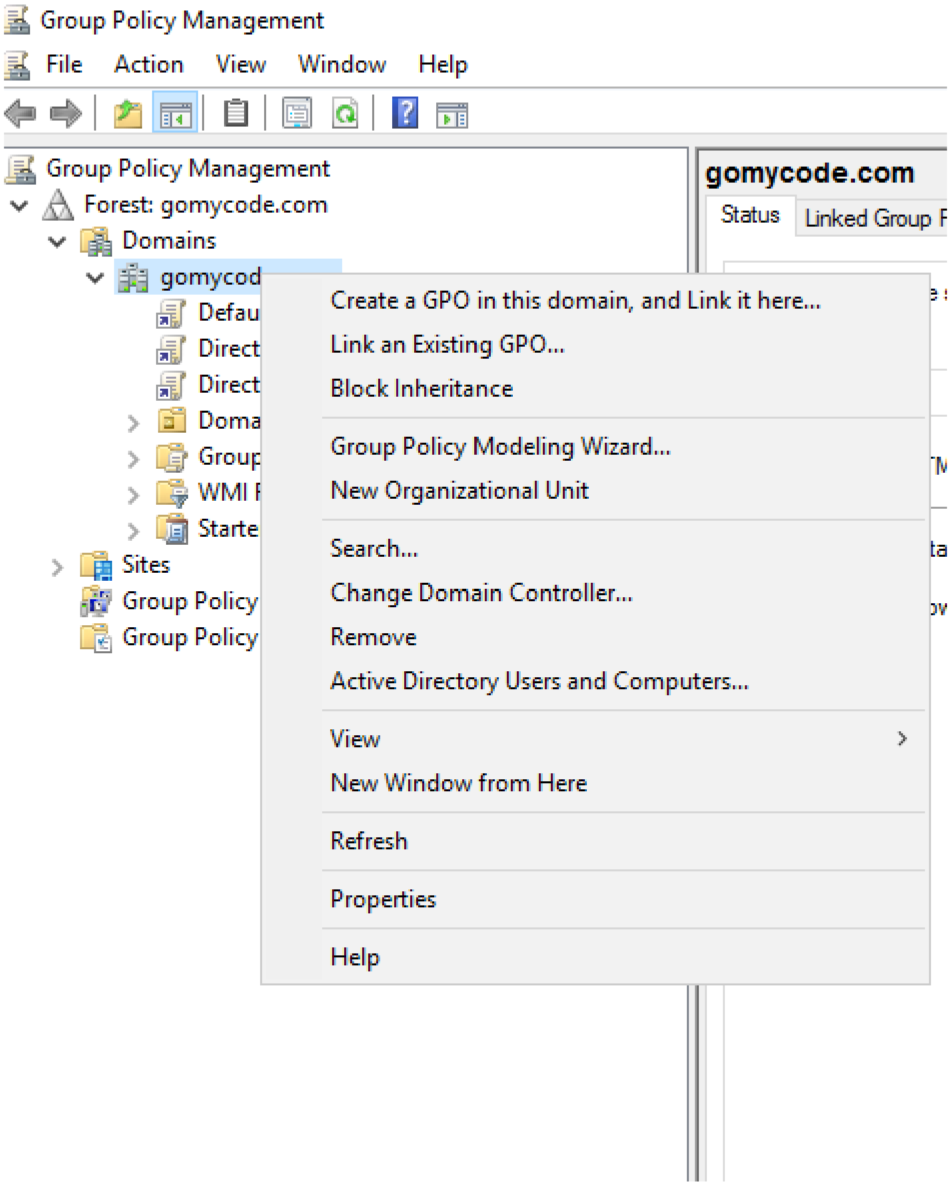
- hit **OK**
- **confirm with okay**
- **we can see that the policy was added to the gomycode (local)**



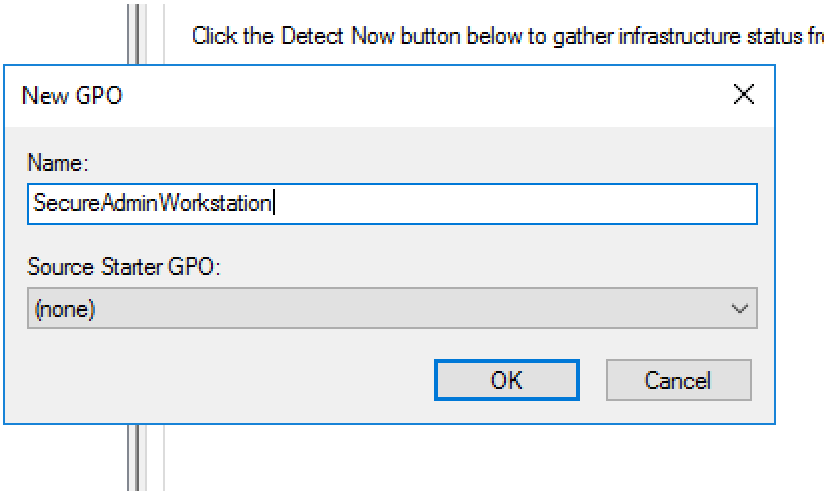
Name	Precedence	Type	Description
Gomycode Account Policy	10	Password S...	

- Now let’s try to add a group Policy

go to **tools** → **group policy management** :



Name the GPO : **SecureAdminWorkstation** :

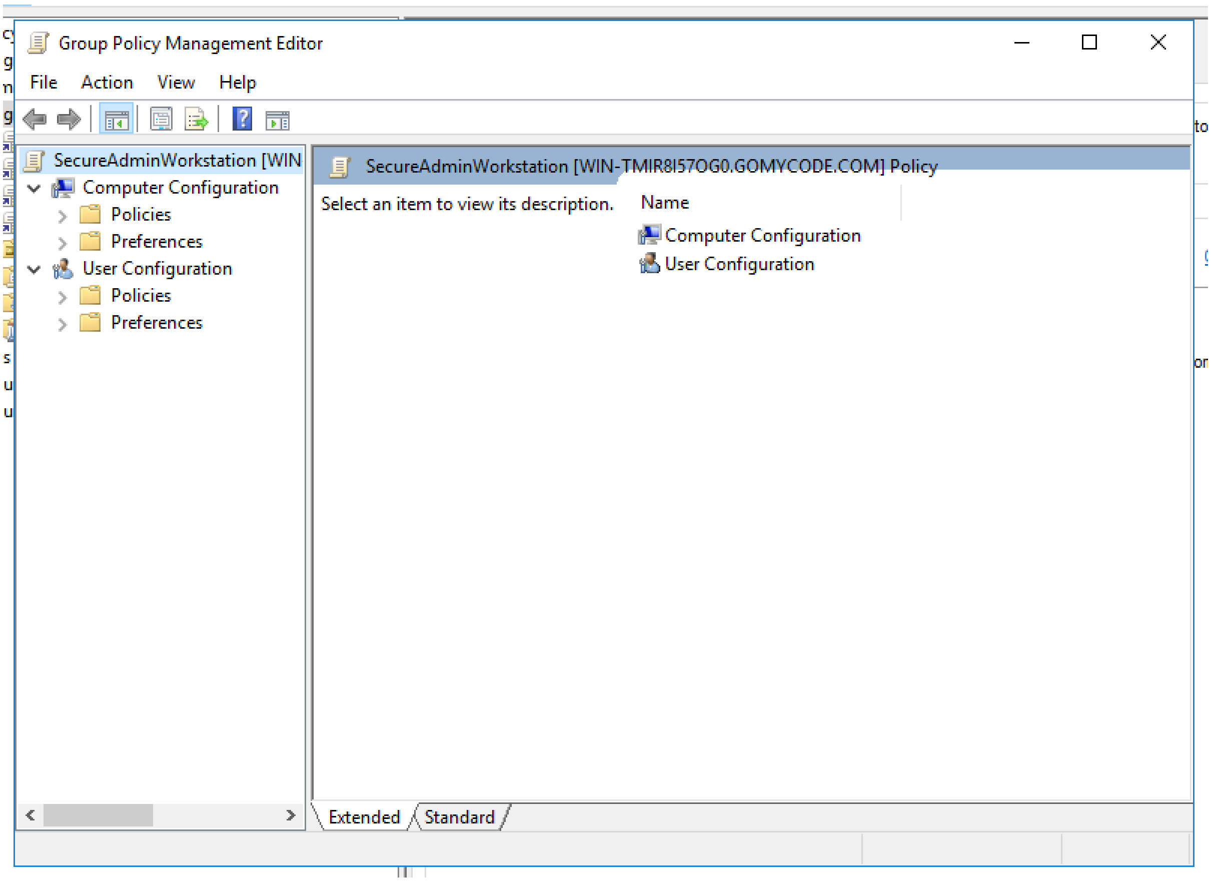

Click the Detect Now button below to gather infrastructure status fr

New GPO

Name: SecureAdminWorkstation

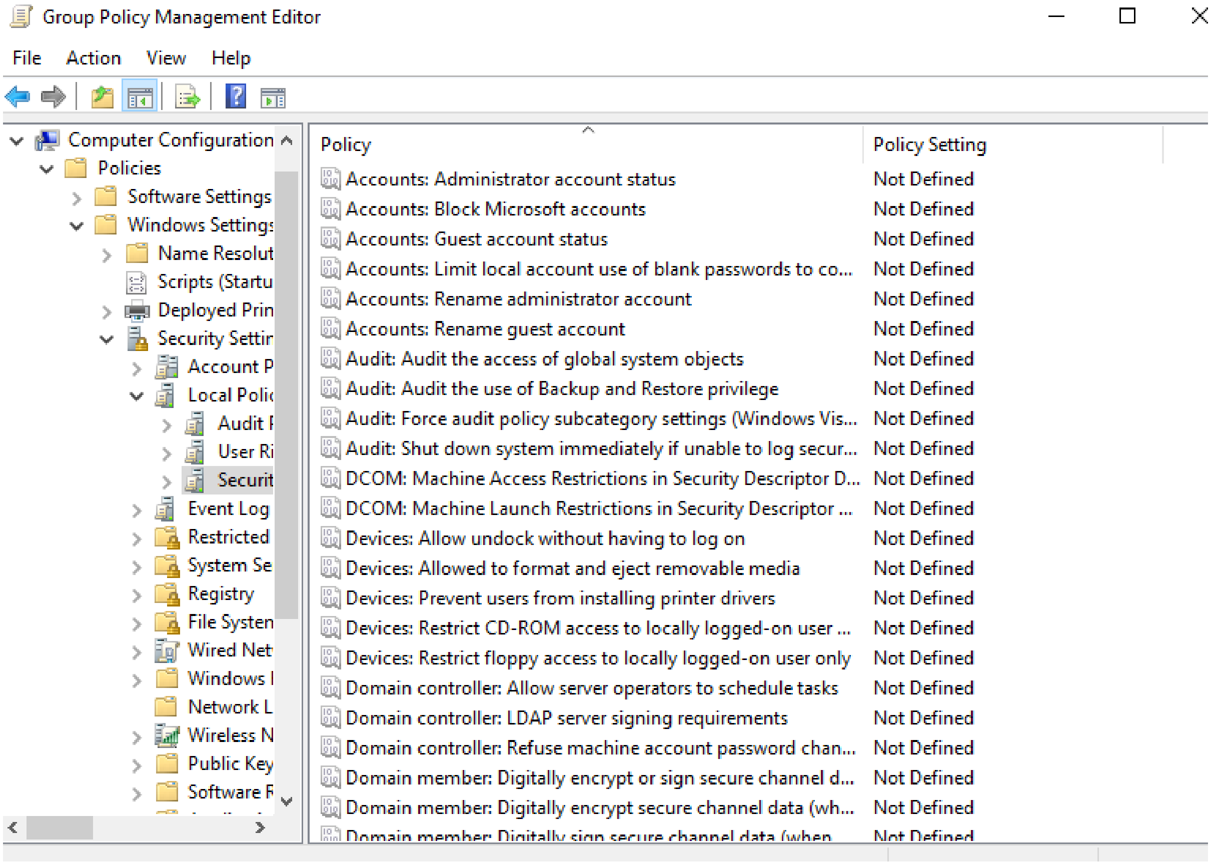
Source Starter GPO: (none)

Edit the GPO : (right click + edit):



Group Policy Management Editor
File
Action
View
Help
SecureAdminWorkstation [WIN
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
SecureAdminWorkstation [WIN-TMIR8I57OG0.GOMYCODE.COM] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard

- Select **Computer Configuration → Policies → Windows Settings → security settings → Local Policies →Security Options :**



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when	Not Defined

- **Now you can disable Guest Accounts**
- change the Administrator account
- choose to not display the last user name in an interactive log-on

(and a lot more)