

PRÁTICA LABORATORIAL 06

Objetivos:

- Políticas de Domínio

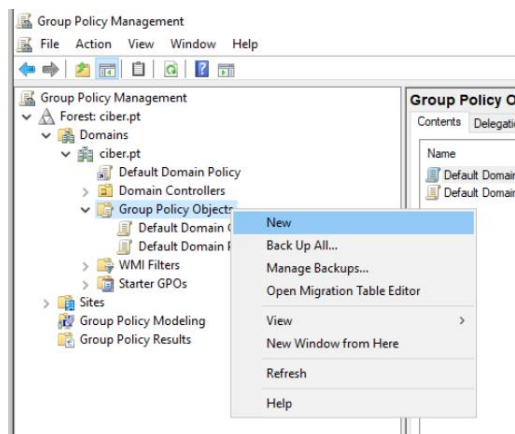
Criar políticas de domínio

Políticas de domínio são idênticas às políticas locais com a diferença que são aplicadas a todo o domínio AD. Isso faz com que a gestão do nosso domínio seja mais simples e eficiente.

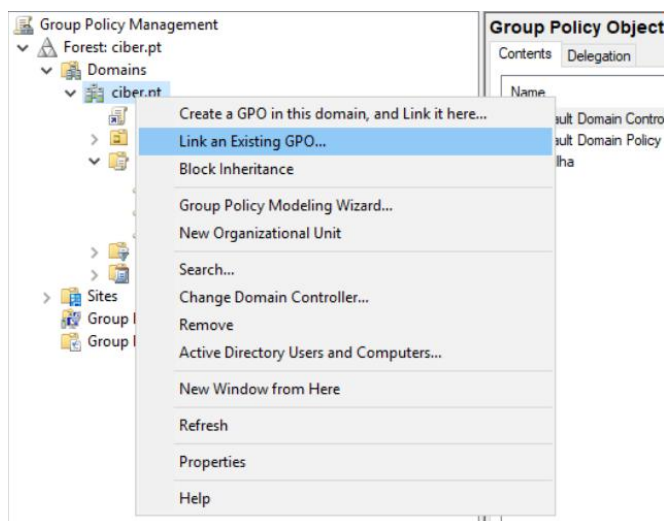
A gestão pode ser feita a partir da janela “Group Policy Management” que encontramos nas ferramentas administrativas. As novas políticas devem ser criadas clicando com o botão direito do rato em [Group Policy Objects] – [New] e escolher o nome que queremos dar à política.

O recomendado é que uma política tenha uma ou poucas regras de forma a tornar as mesmas mais eficientes no caso de queremos aplicar políticas diferentes a grupos ou utilizadores diferentes.

A **Default Domain Policy** nunca deve ser alterada a não ser para efeitos de Account Policies: Password Policy, Account Lockout Policy e Kerberos Policy.

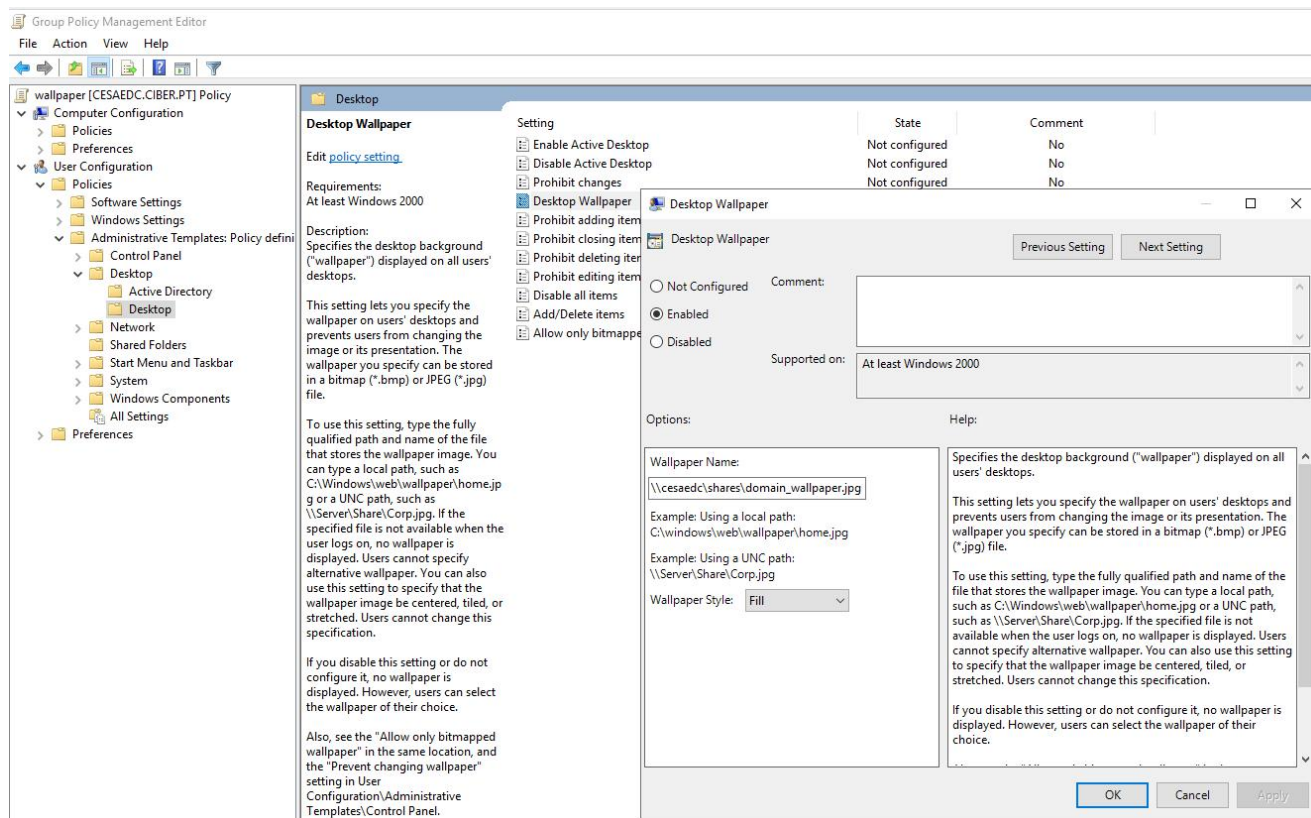


Depois de atribuir um nome à política e fazer a sua configuração [Edit], para que ela fique ativa no domínio temos de clicar com o botão direito em cima do domínio e clicar em [Link an existing GPO ...] e escolher a gpo que queremos ativar:



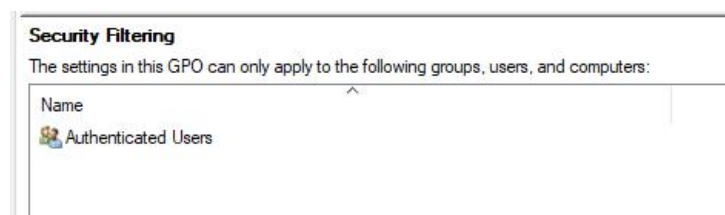
Forçar desktop wallpaper

Para forçar o mesmo desktop wallpaper para todos os utilizadores, editamos a política e [User Configuration] – [Policies] – [Administrative Templates ...] - [Desktop] e clicamos em [Desktop Wallpaper]. Podemos escolher um wallpaper local ou numa drive de rede:

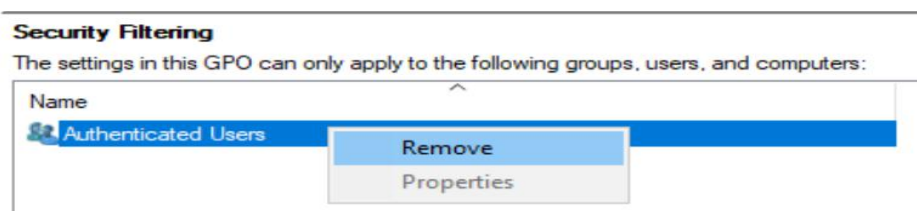


Aplicar GPO apenas a alguns utilizadores ou grupos

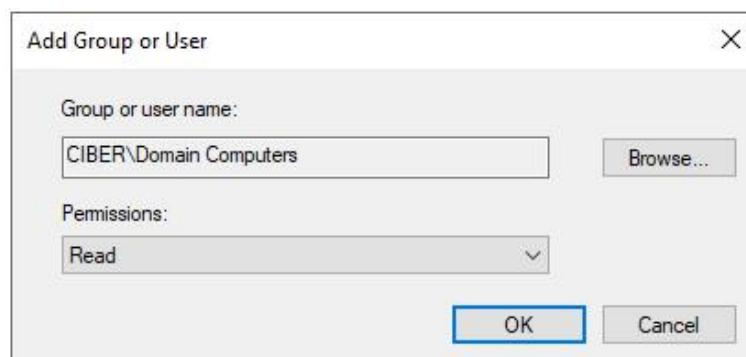
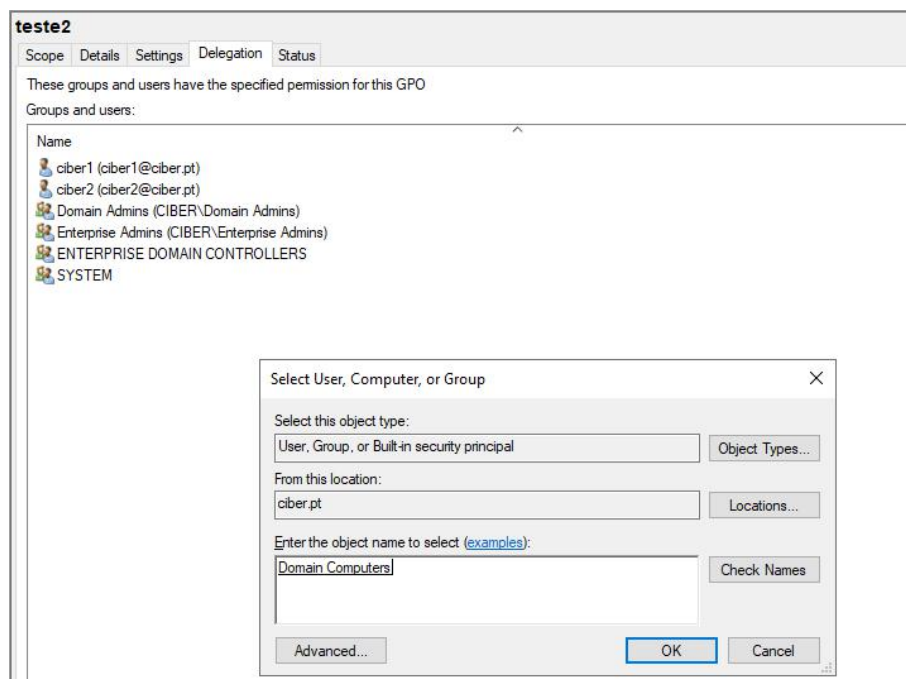
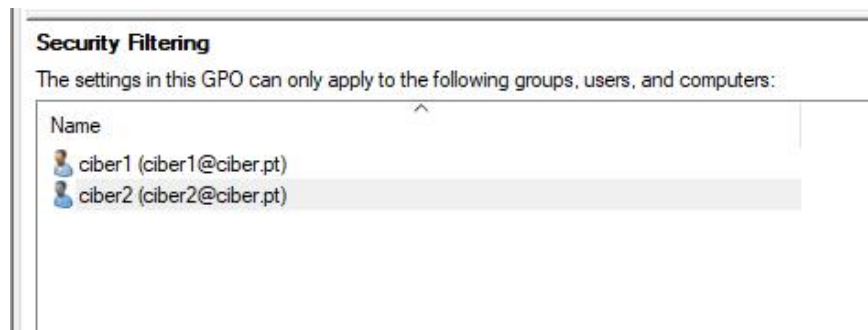
Por defeito as políticas são aplicadas a todos os utilizadores autenticados. Quando clicamos na GPO após a criação em Security Filtering fica automaticamente Authenticated Users:



Se quisermos aplicar a GPO apenas a alguns utilizadores a grupos temos de remover os Authenticated Users:

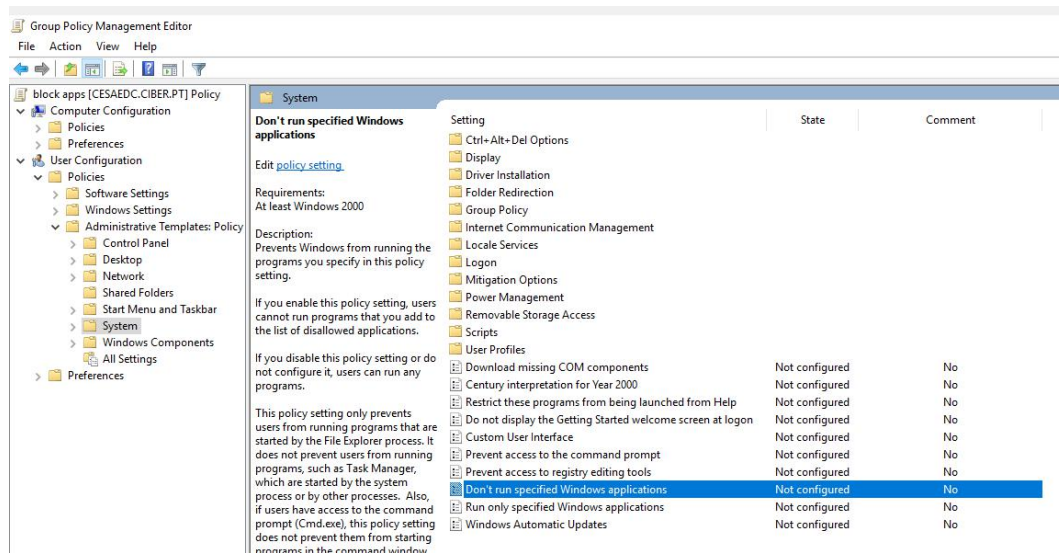


De seguida adicionamos os utilizadores pretendidos e no tab [Delegation] temos de adicionar o grupo **Domain Computers** com permissões de leitura:

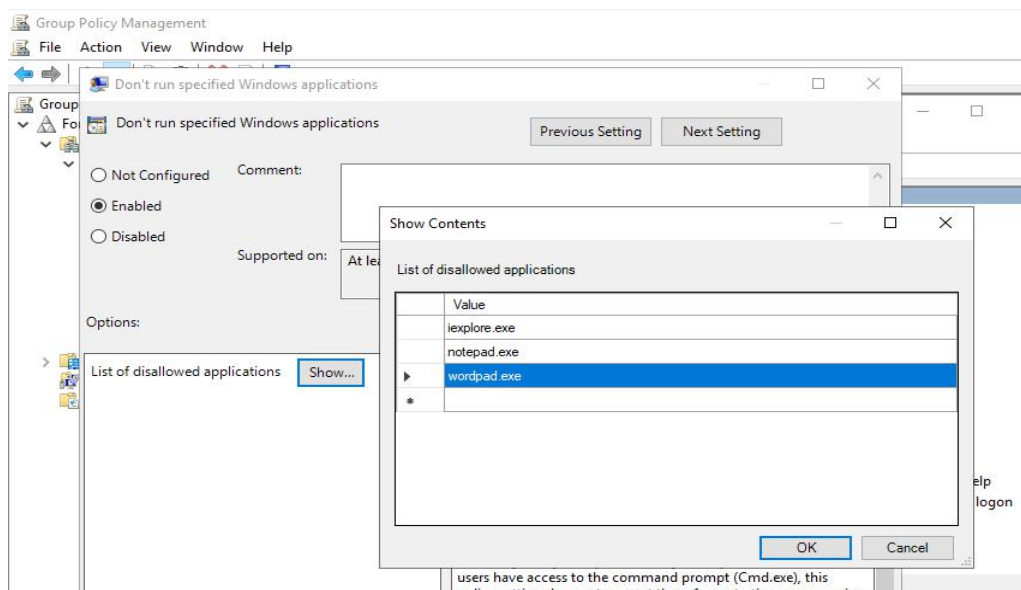


Aplicar GPO para impedir a utilização de algumas aplicações

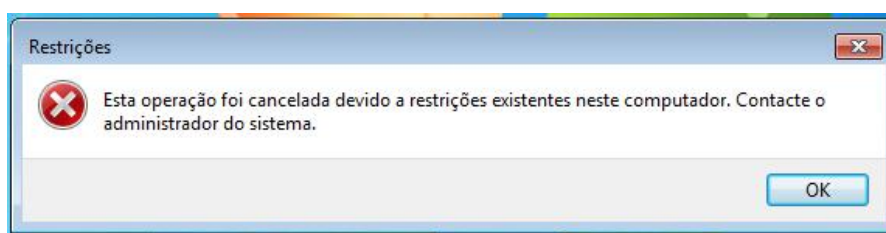
[User Configuration] – [Policies] – [Administrative Templates] – [System] e clicar em [Don't run specified Windows applications]:



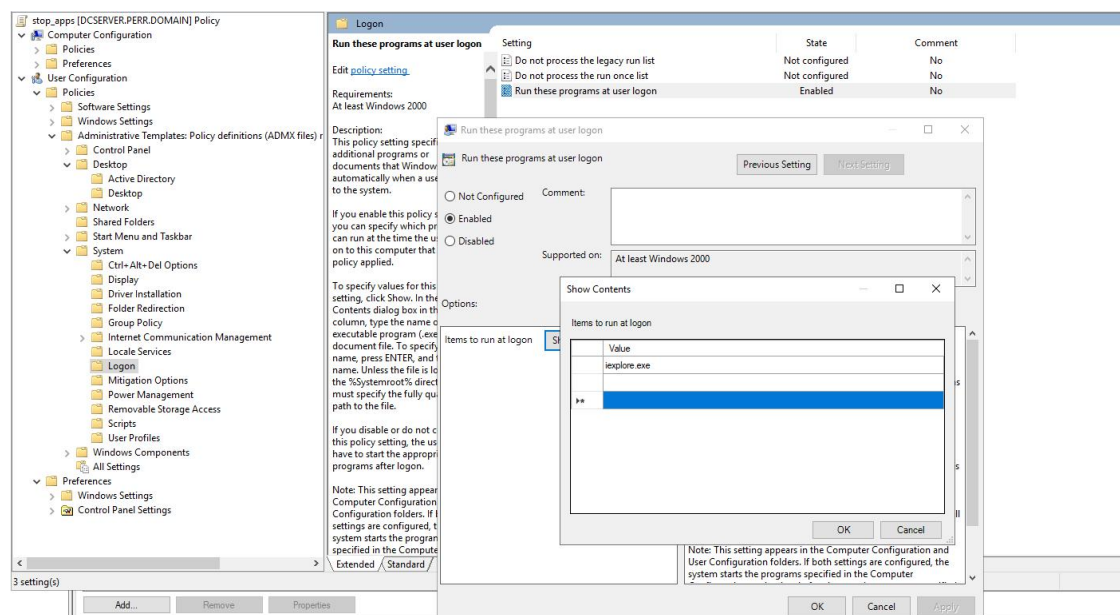
Alterar o estado para [Enabled] e clicar no botão [Show...] Aqui teremos de colocar o nome do executável das aplicações que queremos restringir, neste caso vamos restringir o internet explorer (iexplore.exe), o notepad (notepad.exe) e Wordpad (wordpad.exe):



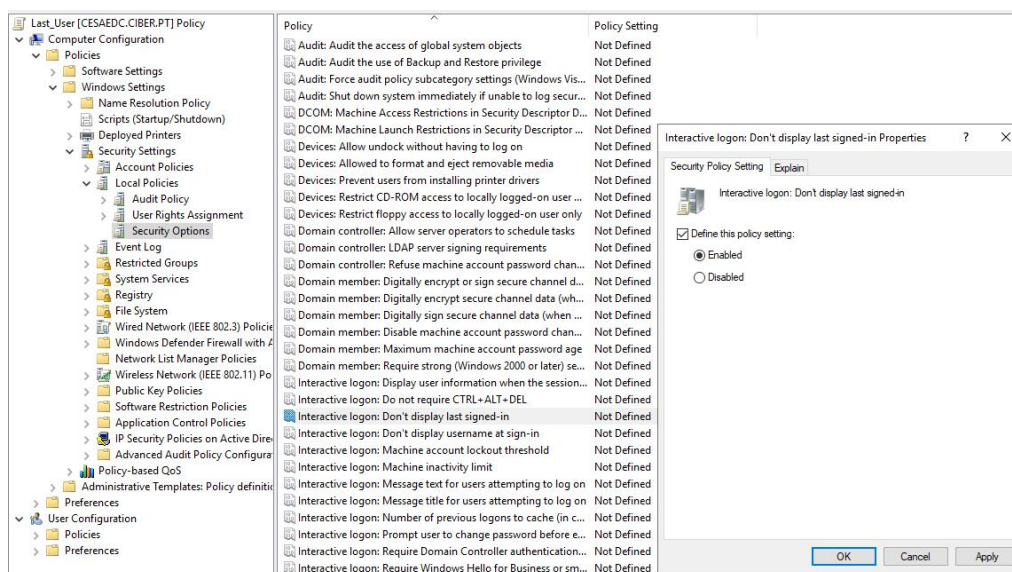
Depois de aplicar a política, as aplicações já não deverão poder ser utilizadas:



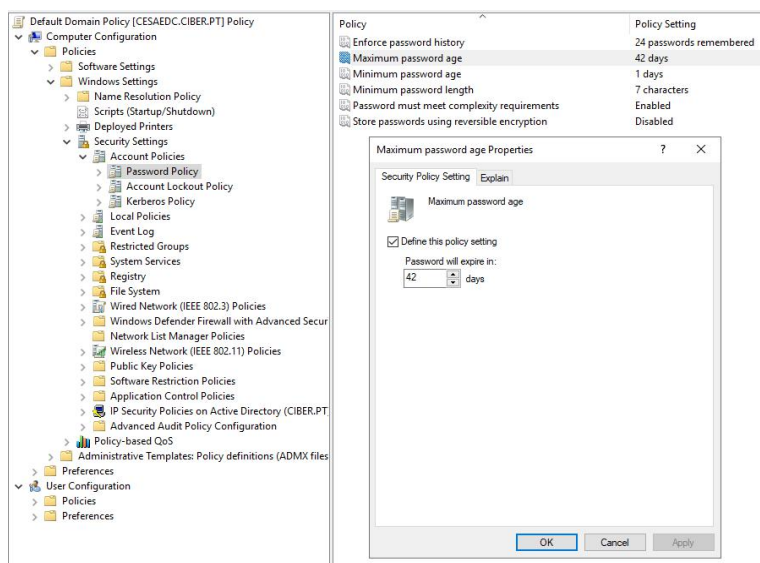
Aplicar GPO para abrir automaticamente aplicações quando o utilizador faz login



Aplicar GPO para não mostrar o último utilizador que fez login

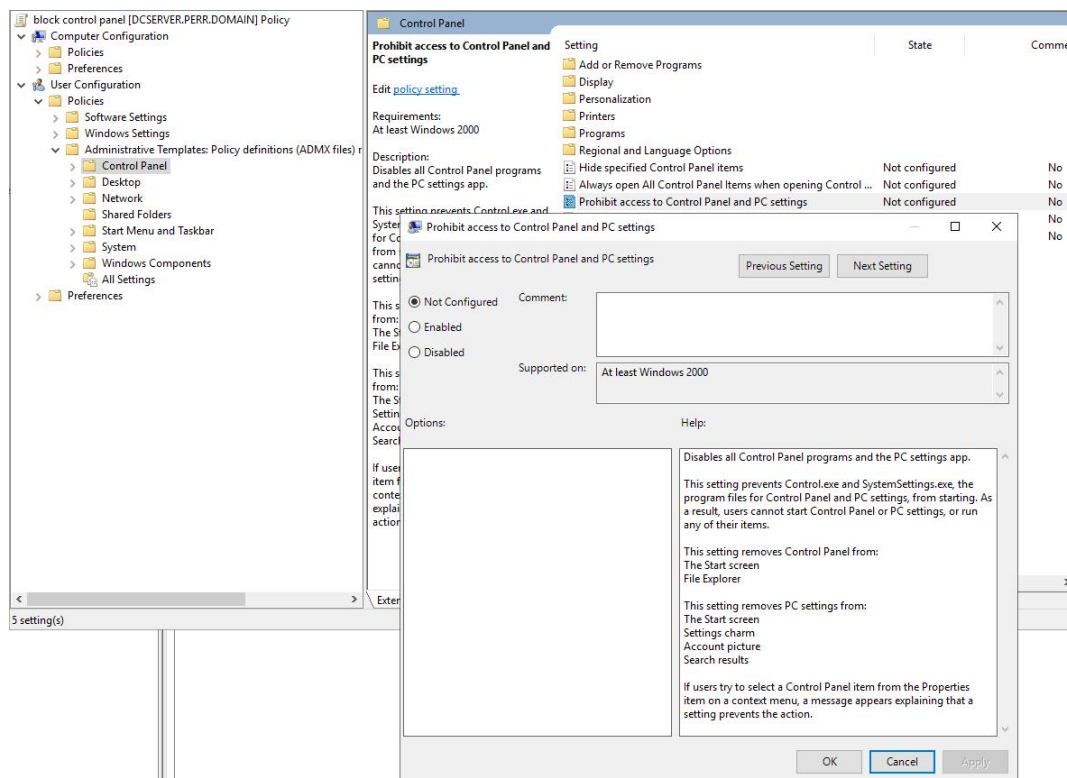


Aplicar GPO para forçar os utilizadores a alterar a password periodicamente – Editar Default Domain Policy



Aqui também é possível definir o tamanho da password a utilizar pelos utilizadores (Minimum password length) ou forçar os utilizadores a utilizar passwords complexas com os requisitos normais do Windows Server (Passwords must meet complexity requirements).

Aplicar GPO para impedir utilizadores de aceder ao painel de controlo



EXERCÍCIOS

1. Crie no Windows server as contas user1, user2, user3 e user4 com a password cesae+123
2. Importe uma máquina cliente (windows 7 ou windows 10) e coloque-a no domínio do servidor usado na questão anterior.
3. Crie os grupos de utilizador gr1 e gr2. Adicione os utilizadores user1 e user2 ao grupo gr1 e o utilizador user3 ao grupo gr2
4. Crie uma política de grupo chamada setpaper que coloque o mesmo wallpaper para todos os utilizadores de domínio.
5. Crie uma política de grupo chamada block apps que não deixe os utilizadores do grupo gr1 de abrir as aplicações edge e notepad.
6. Altere a política anterior para que a aplicação notepad abra automaticamente sempre que os utilizadores do grupo gr1 façam login.
7. Crie uma política de grupo chamada blockcontrolpanel para que os utilizadores user2 e user3 não possam abrir o painel de controlo.
8. Crie uma política com o nome alerts_login que indique aos utilizadores uma mensagem a alertar para o facto de terem a conta bloqueada caso falhem a password três vezes.
9. Altere a política anterior de forma a forçar os utilizadores a ter de executar a combinação de teclas CTRL+ALT+DEL antes de fazer login.
10. Faça as alterações necessárias para que o login dos utilizadores seja bloqueado durante 60 min, caso errem a password 3 vezes.

DICA: <https://techexpert.tips/windows/gpo-prevent-access-control-panel/>

Bom trabalho!