

GlobalTcert.com

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

QUESTION 2

You are the network administrator for GlobalitcerT . The network consists of a Windows 2000 Active Directory domain. The network contains three Windows 2000 Server computers that are configured as domain controllers and Windows 2000 Professional client computers.

Your manager receives a new security template named Lockout.inf. Your manager asks you to ensure that the Account Lockout Policy for the domain is not less secure than that of the Local.inf policy. You run the Security Configuration and Analysis console on a domain controller. You use Lockout.inf to analyze the domain controller security settings.

You review the Account Lockout Policy of the analysis. The following table shows the relevant portion of the analysis

| Policy Database Setting | Computer Setting |
|-------------------------------------|---|
| Account lockout duration | 0 minutes 45 minutes |
| Account lockout threshold | 5 invalid logon attempts 4 invalid logon attempts |
| Reset account lockout counter after | 20 minutes 30 minutes |

You need to increase the security of the Account Lockout Policy of the domain in all areas in which it is less restrictive than the Lockout.inf template.

What should you do?

- A. Import the Lockout.inf template to the Domain Security Policy.
- B. Import the Lockout.inf template to the Domain Controller Security Policy.
- C. Configure the Account lockout duration portion of the Domain Security Policy for 0 minutes.
- D. Configure the Reset account lockout counter after portion of the Domain Security Policy for 20 minutes.
- E. Configure the Account lockout threshold portion of the Domain Controller Security Policy for 5 invalid logon attempts.

Answer: C

QUESTION 3

You are the administrator of GlobalitcerT .com network which consists of a single Active Directory domain. The network serves 10 sites and a total of 1500 client computers all running Windows 2000 Pro. Users are not local administrators of their own computers.

Your IT department issues new business rules. The following requirements now apply to all client computers:

- Passwords must meet requirements for complexity. The computer browser service must be disabled. Only domain users must be able to access their computers remotely when they use a VPN to connect to the network.

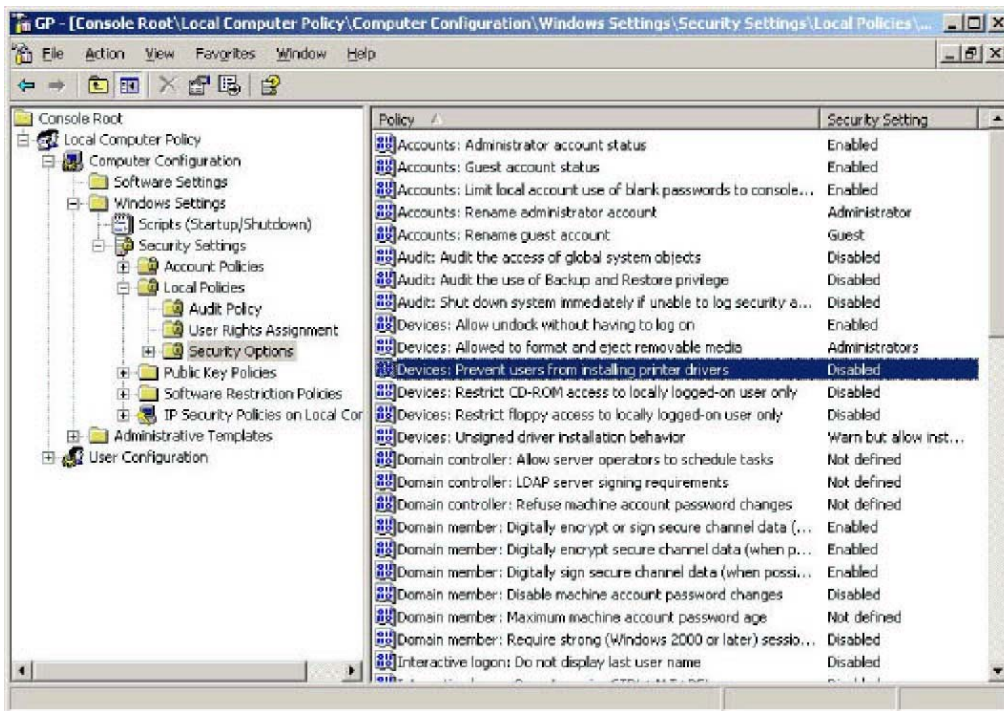
Users must not be able to install printer drivers.

You create a GPO named Computer Setting to enforce these business rules.

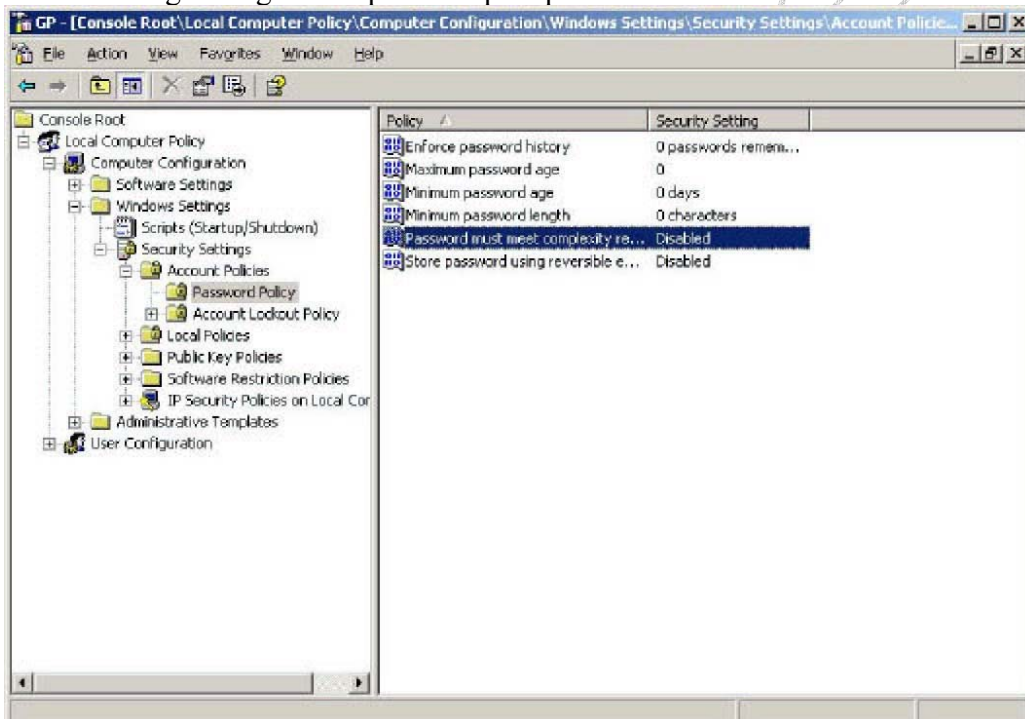
Click on the right sections into the computer settings security policy.

Answer:

The following setting will prevent users installing printer drivers.



The following setting will require complex passwords.



QUESTION 4

You are the administrator of GlobalitcerT 's Windows 2000 network. You implement company security policies by using the Security Configuration and Analysis snap-in on each domain controller.

The password security policy forces all users to change their passwords every five weeks. The policy also

prevents users from reusing their last seven passwords. Server users in the domain can bypass this policy by changing a password seven times and then changing it back to the original password.

You change all users' passwords so that they are at least eight characters long. You must ensure that users cannot bypass the policy. You also need to make sure that the template prevents users from reusing the same password for at least five weeks.

You want to configure the password security template to support these requirements. What should you do?

- A. Set the minimum password age to 6 days.
- B. Set the maximum password age to 42 days.
- C. Enable password complexity requirements.
- D. Disable the storage of passwords in reversible encryption.

Answer: A

Explanation: With a minimum password age of 6 days, the server users would be able to change the password a maximum of 7 times in 5 weeks. For example 1st day, 6th day, 11th day, 16th day, 21st day, 26th, and 31st day.

The eighth time would be outside the 5 week period.

Incorrect Answers

B: Changing the maximum password age to 42 days does not help achieving the requirements. Server users would still be able to change passwords as often they wanted and thus be able to reuse passwords frequently. Furthermore, the restriction to change password every 5 weeks is changed to every 6 weeks instead.

C: There is no requirement to meet any complexity requirement of the passwords.

D: The Store Password Using Reversible Encryption For All Users In The Domain option is useful with the Challenge Handshake Authentication Protocol (CHAP). It would be of no use in this scenario, however.

QUESTION 5

You are the administrator of GlobalitcerT .com's network. The network is configured as a Windows 2000 domain.

You want to strengthen the security of communications between client computers and servers in the Reps organizational unit (OU). You do not want to decrease overall productivity of the domain.

What should you do?

- A. Create one Group Policy object (GPO) in the Sales OU. Increase maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.
- B. Create one Group Policy object (GPO) in the Sales OU. Decrease maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.
- C. Create one Group Policy object (GPO) in the Reps OU. Decrease maximum service ticket lifetime in the GPO, and increase maximum lifetime that a user ticket can be renewed in the GPO.
- D. Create one Group Policy object (GPO) in the Reps OU. Decrease maximum service ticket lifetime in the GPO, and decrease maximum lifetime that a user ticket can be renewed in the GPO.

Answer: C