

# 70-214

## Microsoft

### *Implementing and Administering Security in a Microsoft*

Visit: <http://www.pass4sureofficial.com/exams.asp?examcode=70-214>

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your 70-214 exam in first attempt, but also you can get a high score to acquire Microsoft certification.

If you use pass4sureofficial 70-214 Certification questions and answers, you will experience actual 70-214 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Microsoft exam prep covers over 95% of the questions and answers that may be appeared in your 70-214 exam. Every point from pass4sure 70-214 PDF, 70-214 review will help you take Microsoft 70-214 exam much easier and become Microsoft certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Microsoft 70-214 course:

- \* Up-to-Date Microsoft 70-214 questions taken from the real exam.
- \* 100% correct Microsoft 70-214 answers you simply can't find in other 70-214 courses.
- \* All of our tests are easy to download. Your file will be saved as a 70-214 PDF.
- \* Microsoft 70-214 brain dump free content featuring the real 70-214 test questions.

Microsoft 70-214 certification exam is of core importance both in your Professional life and Microsoft certification path. With Microsoft certification you can get a good job easily in the market and get on your path for success. Professionals who passed Microsoft 70-214 exam training are an absolute favorite in the industry. You will pass Microsoft 70-214 certification test and career opportunities will be open for you.



**QUESTION 1:**

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain named Certkiller .com.

You have deployed a new Windows 2000 Server computer as a Web server in the perimeter network (also known as the DMZ). The Web server is not a member of Certkiller .com. A firewall between the network and the DMZ is configured to allow only HTTP traffic to be sent from the DMZ to the private network.

Your Web server administrator creates a security template named Webserver.inf that defines the default security settings required for the Web server. The security template settings must be enforced at the Web server and applied at regular intervals.

What should you do?

A. Make the Web server a member of the Certkiller .com domain and place the Web server computer account into a new organizational unit (OU).

Import the Webserver.inf security template to the Default Domain Policy.

B. Create a batch file that applies the security template by using the `secedit /configure /cfg Webserver.inf /db web.sdb` command.

In Scheduled Tasks, create a new task to run the batch file daily.

C. Apply the security template using the Security Configuration and Analysis console on the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

D. Import the Webserver.inf security template to the Local Computer policy of the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

Answer: C

Explanation:

We apply the security template using the Security Configuration and Analysis console.

We then update the security policy at regular intervals using a scheduled task.

Incorrect Answers

A: We do not want to apply the Webserver.inf to all computers in the domain.

B: We do repeatedly have to apply the security template.

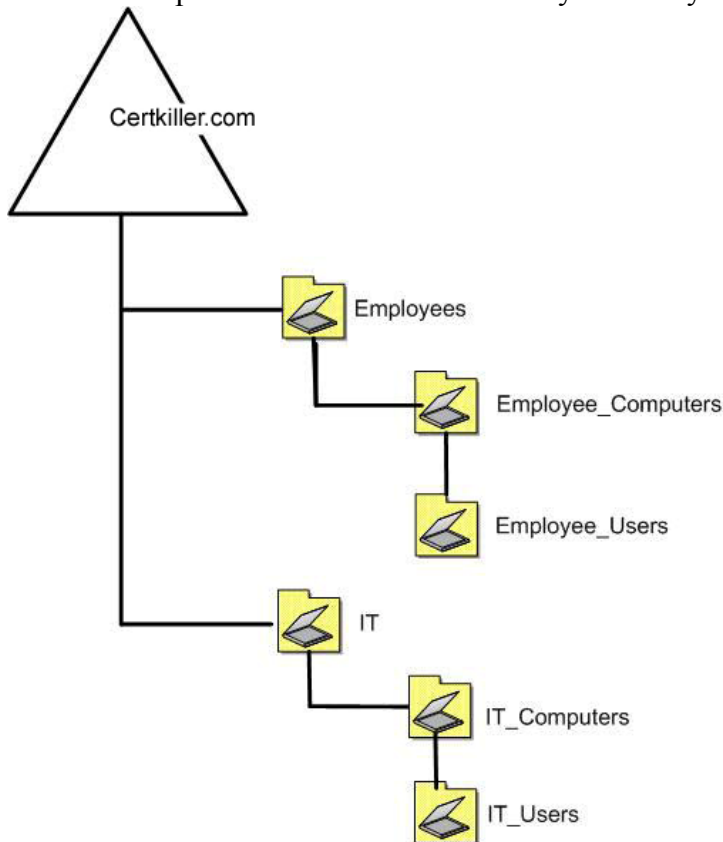
D: The initial template applied to a computer is called the Local Computer Policy. It is not a good practice to change this template.

---

**QUESTION 2:**

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain

controllers and 500 Windows 2000 Professional computers.  
The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The user accounts for all administrators are located in the IT\_Users organizational unit (OU). All other user accounts are located in the Employee\_Users OU. The client computer accounts for the administrators' computers are located in the IT\_Computers OU. All other client computer accounts are located in the Employee\_Computers OU. Your company employs 10 security auditors to ensure that servers and client computers comply with the written security policy of Certkiller. You create a domain security group named Security\_Audit. You add the computer accounts for each security auditor to this group.

You create several Group Policy objects (GPOs) and link them to the Employees OU. The GPOs configure security settings to enforce the written policy. The priority and configuration of each GPO are shown in the following table.

GPO name	Policy	Setting	Object with Read and Apply Group Policy Permissions	Priority	No Override
GPO1	Audit object access	Success and Failure	AuthenticateUsers Security_Audit	1	
GPO2	Audit logon	Failure	Security_Audit	2	

	events				
GPO3	Audit account logon events	Success	AuthenticateUsers Security_Audit	3	X

You discover that the Security logs on many client computers are full of successful object access events from the users of the client computers. You do not want users to be audited when they access files on their own computers. However, you want the security auditors to be audited when they access any file on any client computer. What should you do?

- A. Clear the No Override check box in GPO3.
- B. Remove the Authenticated Users group from the DACL for GPO1.
- C. Configure the policy settings for GPO3 so that success and failure events are audited.
- D. Configure the DACL for GPO1 so that the Authenticated Users group has Deny - Apply Group Policy permission.

Answer: B

Explanation:

By removing the Authenticated Users group from the DACL of GPO1, only members of the Security\_Auditgroup would be audited for Object Access.

Incorrect Answers

A, C: GPO1 would still be applied, and object Access by the Authenticated Users group would still be audited.

D: The auditors, like all users, belong to the Authenticated Users group. They would also be receive Deny - Apply Group Policy permission, and they would not be audited contrary to the requirements in this scenario.

---

### QUESTION 3:

You are the network administrator for Certkiller . The network consists if a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers and 50 Windows NT Workstation 4.0 computers.

You perform a clean installation of Windows 2000 Professional on four client computers. You do not install Internet Information Services (IIS) on these computers.

The written security policy for Certkiller allows Windows 2000 Professional users to install and run IIS. Every computer running IIS must be configured to meet the written policy before the computer can be connected to Certkiller network.

You want to ensure that the written policy for IIS is enforced automatically if IIS is installed on a Windows 2000 Professional computer.

What should you do before the user receive their computers?

## 070-214

- A. On each Windows 2000 Professional computer, modify the Ocfilsw.inf security template to comply with the written policy.
- B. On each Windows 2000 Professional computer, modify the Setup Security.inf security template to comply with the written policy.
- C. On a reference computer, configure IIS permissions to comply with the written policy. In the local Group Policy editor, select Import current Authenticode Security information. Select the Export Browser Settings option and save the settings to a file. Place the file in Systemroot\System32 on each Windows 2000 Professional computer.
- D. On a reference computer, configure IIS permissions to comply with the written policy. In the local Group Policy editor, select Import current security zones settings. Select the Export List option and save the list to a file. Place the file in Systemroot\System32 on each Windows 2000 Professional computer.

Answer: C

### Explanation:

You can use Authenticode to designate software publishers and credentials agencies as trustworthy. You can also import these settings from your computer. If you want to modify the settings that you will apply to your users' computers, click Import current Authenticode security information, and then click Modify Settings.

Authenticode allows administrators to designate software publishers and credentials agencies as trustworthy. These settings can also be imported from the administrator's computer. Click Import current Authenticode information, and then click Modify Settings to modify the settings that will apply to users' computers.

### Incorrect Answers

A: It would be a daunting administrative task to reconfigure each client computer manually. Furthermore, the OCFiles.inf file defines Optional component file security for Professional.

B: It would be a daunting administrative task to reconfigure each client computer manually. Furthermore, the secure templates (secure\*.inf) implement recommended security settings for all security areas except files, folders, and registry keys.

D: IIS security does not primarily concern accessing secure sites.

---

## **QUESTION 4:**

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains 2,000 portable computers that run Windows XP Professional. All portable computers use Microsoft Internet Explorer as their only Web browser.

When you work from home, your portable computer automatically dials in to Certkiller network so that you can administer network resources remotely. The written security policy for Certkiller requires stricter security zone and privacy settings for all portable computers. You configure your portable computer to comply with the written policy. You create a Group Policy object (GPO) named SetSecurity and link it to the domain. You import the connection settings from your computer to the Security Zones and

Content Ratings policy in SetSecurity.

Now, when other users work from home, they report that their computers attempt to dial in to Certkiller network automatically. However, the connections fail because only administrators have dial-up permissions to Certkiller network.

You need to restore the dial-up configuration for other users to its previous state, while continuing to enforce the written security policy.

What should you do?

- A. On your portable computer, open the Programs policy in the Internet Explorer maintenance section of the SetSecurity GPO, and select the option to import settings. Save the modified GPO.
- B. On your portable computer, modify the Automatic Browser Configuration policy of the SetSecurity GPO so that automatic browser configuration is disabled. Save the modified GPO.
- C. Delete, re-create, and then link the SetSecurity GPO to the domain by using a Windows XP Professional computer that has the same configuration as your portable computer.
- D. Create a new user account in the domain. Use the new account to log on to your portable computer. Configure the settings to comply with the written policy, configure the dial-up configuration to not dial, and import those settings to the SetSecurity GPO. Delete the new user account.

Answer: D

Explanation:

The administrator account was used when configuring the LapTop computers. Administrators are allowed to connect remotely. We must therefore use a non-administrator user account when configuring the GPO that should be used on the LapTops.

Incorrect Answers

A: An incomplete solution.

B: The Automatic Browser Configuration policy is used to automatically push the updated security zone settings to each user's desktop computer, enabling the administrator to manage security policy dynamically across all computers on the network.

C: We need to configure the template with a NON admin account

---

## QUESTION 5:

You are the network administrator for Certkiller . The network consists of a Windows 2000 Active Directory domain. The domain contains domain controllers that run either Windows 2000 Sever or Windows NT Server 4.0.

You need to modify a registry entry on all domain controllers. You create an administrative template that contains the registry entry. You need to apply the template only to each domain controller every time it is restarted.

## Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time \$99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads

<http://www.pass4sureofficial.com/allexams.asp>

View list of All Study Guides (SG) downloads

<http://www.pass4sureofficial.com/study-guides.asp>

View list of All Audio Exams (AE) downloads

<http://www.pass4sureofficial.com/audio-exams.asp>

Download All Exams Samples

<http://www.pass4sureofficial.com/samples.asp>

To purchase \$99 Lifetime Full Access Membership click here

<http://www.pass4sureofficial.com/purchase.asp>

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA	

