VCE & PDF
GeekCert.com

70-688^{Q&As}

70-688^{Q&As}

Supporting Windows 8.1

Pass Microsoft 70-688 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/70-688.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Your company has several Windows RT 8.1 devices. The devices connect to Exchange Online in Microsoft Office 365 and to Windows Intune for device management.

Setting name	Local device setting	Windows Intune setting	Exchange Online setting
Require a password to unlock mobile devices	Not configured	Yes	No
Required password type	Not configured	Aplhanumeric	Numeric
Minimum password length	Not configured	10	12
Allow simple passwords	Not configured	No	Yes
Minutes of inactivity before device screen is locked	Not configured	10	5

The security policies of Office 365 and Windows Intune are configured as shown in the following table.

You need to identify the effective settings on the Windows RT devices.

What should you identify? (To answer, select the appropriate effective configuration for each setting in the answer area.)

Answer Area

Require a password to unlock mobile devices: [▼]

Required password type: [▼]

Minimum password length: [▼]

Allow simple passwords: [▼]

Minutes of inactivity before device screen is locked: [▼]

Hot Area:

Answer Area

Require a password to unlock mobile devices:

| Yes |
| No |
| Not configured |

Required password type:

| Alphanumeric |
| Numeric |
| Not configured |

Minimum password length:

| 10 |
| 12 |
| Not configured |

Allow simple passwords:

| Yes |
| No |
| Not configured |

Minutes of inactivity before device screen is locked:

| 5 |
| 15 |
| Not configured |

Correct Answer:

Answer Area

Require a password to unlock mobile devices:
- Yes
- No
- Not configured

Required password type:
- Alphanumeric
- Numeric
- Not configured

Minimum password length:
- 10
- 12
- Not configured

Allow simple passwords:
- Yes
- No
- Not configured

Minutes of inactivity before device screen is locked:
- 5
- 15
- Not configured

http://technet.microsoft.com/en-us/library/dn283963.aspx

QUESTION 2

Your network contains an Active Directory domain. The domain contains Windows 8.1 Enterprise client computers.

Users frequently use USB drives to store sensitive files that are used on multiple computers.

Your corporate security policy states that all removable storage devices, such as USB data drives, must be encrypted.

You need to ensure that if a user forgets the password for a USB disk that is encrypted by using BitLocker To Go, the user can resolve the issue themself.

What should you do?

A. Instruct the user to open BitLocker Drive Encryption, select Back up recovery key, and then select Save to a file.

B. From an elevated command prompt, run Manage-BDE hangeKey.

C. Instruct the user to open BitLocker Drive Encryption, select Backup Recovery Key, and then select Save to your Microsoft account.

D. For each computer, create a USB startup key.

Correct Answer: C

Explanation: The recovery password and recovery key for an operating system drive or a fixed data drive can be saved to a folder, saved to one or more USB devices, saved to your Microsoft account online, or printed. Microsoft highly recommend that you either store the recovery information in AD DS, along with your Microsoft account online, or another safe location.

Note: A BitLocker recovery key is a special key that you can create when you turn on Bitlocker Drive Encryption for the first time on each drive that you encrypt. You can use the recovery key to gain access to your computer if the drive that Windows is installed on (the operating system drive) is encrypted using BitLocker Drive Encryption and BitLocker detects a condition that prevents it from unlocking the drive when the computer is starting up. A recovery key can also be used to gain access to your files and folders on a removable data drive (such as an external hard drive or USB flash drive) that is encrypted using BitLocker To Go, if for some reason you forget the password or your computer cannot access the drive.

Reference: BitLocker Frequently Asked Questions (FAQ)

https://technet.microsoft.com/en-us/library/hh831507.aspx#BKMK_RecoveryPass

QUESTION 3

You are an application developer for a federal government agency. You maintain a legacy application that the agency originally developed for Windows 2000. The agency is upgrading all desktop computers to Windows 8.1.

The legacy application does not run on Windows 8.1. You use the Application Compatibility Toolkit (ACT) to create a shim.

You need to deploy the shim to all Windows 8.1 computers.

What should you do?

A. Run the sdbinst.exe utility on each computer to install the shim locally.

B. Configure a Group Policy to install the shim with user privileges.

C. Install the shim on all Windows XP computers prior to the Windows 8.1 upgrade.

D. Install the shim with a PowerShell script by using the ACT PowerShell add-in.

Correct Answer: D

Explanation: Deploying a custom shim database to users requires the following two actions:

*

 Placing the custom shim database (*.sdb file) in a location to which the user\\'s computer has access (either locally or on the network)

*

 Calling the sdbinst.exe command-line utility to install the custom shim database locally While any approach that completes these two actions will work, customers commonly use one of the following two approaches:

*

 Packaging the *.sdb file and a script in an .msi file and then deploying the .msi file, making sure to mark the custom action not to impersonate the calling user. For example, if using Microsoft Visual Basic?Scripting Edition (VBScript) script, the custom action type would be msidbCustomActionTypeVBScript + msidbCustomActionTypeInScript + msidbCustomActionTypeNoImpersonate = 0x0006 + 0x0400 + 0x0800 = 0x0C06 = 3078 decimal.

*

 Placing the *.sdb file on a network share, and then calling a script on target computers, making sure to call the script at a time when it will receive elevated rights (for example, from a computer start-up script instead of a user log-in script). Reference: Custom Shim Database Deployment https://technet.microsoft.com/en-us/library/dd837647(v=ws.10).aspx
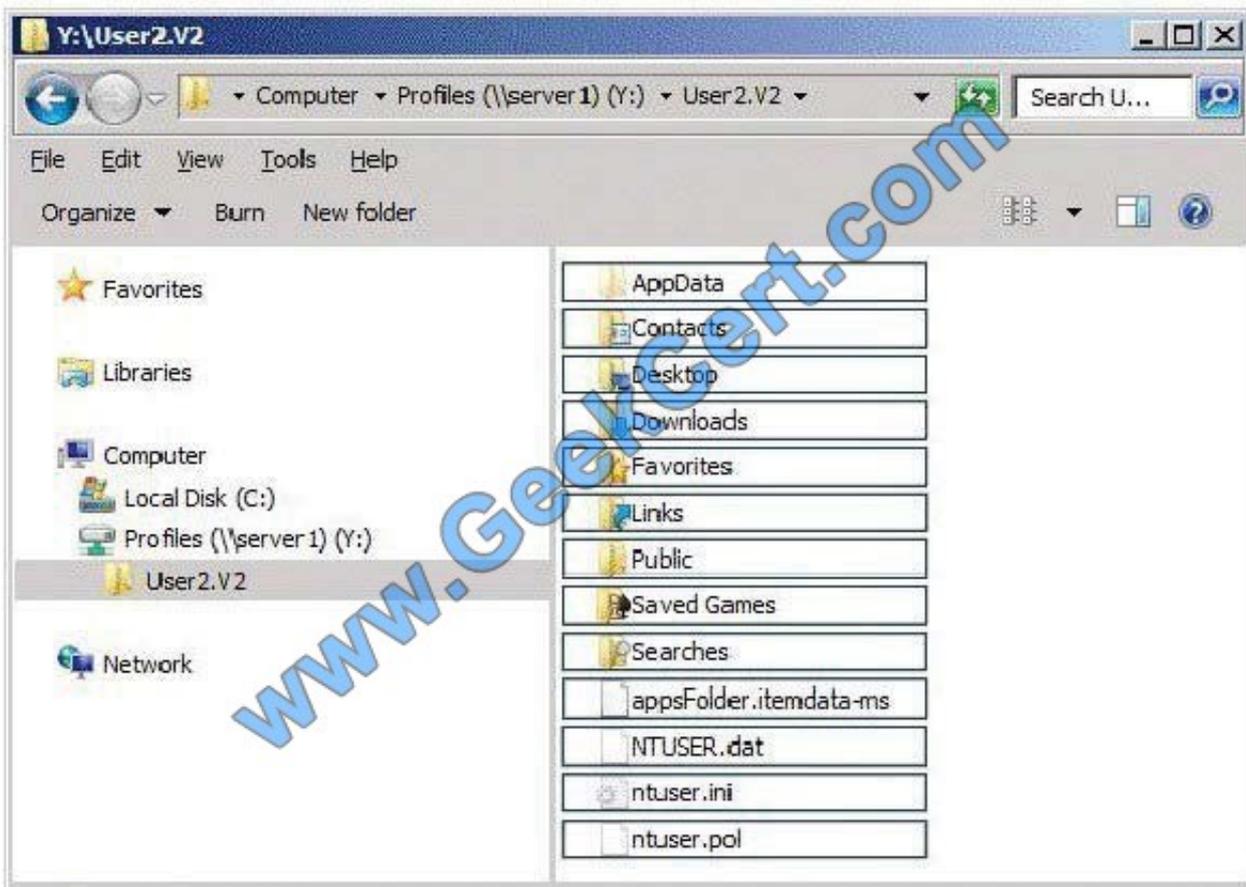
QUESTION 4

Your network contains an Active Directory domain named contoso.com. All client computers in the domain run Windows 8.1 Pro. All domain users have roaming user profiles.

You need to prevent a user named User2 from being able to save changes to his roaming user profile.

Which file or folder should you modify? (To answer, select the appropriate file or folder in the answer area.)
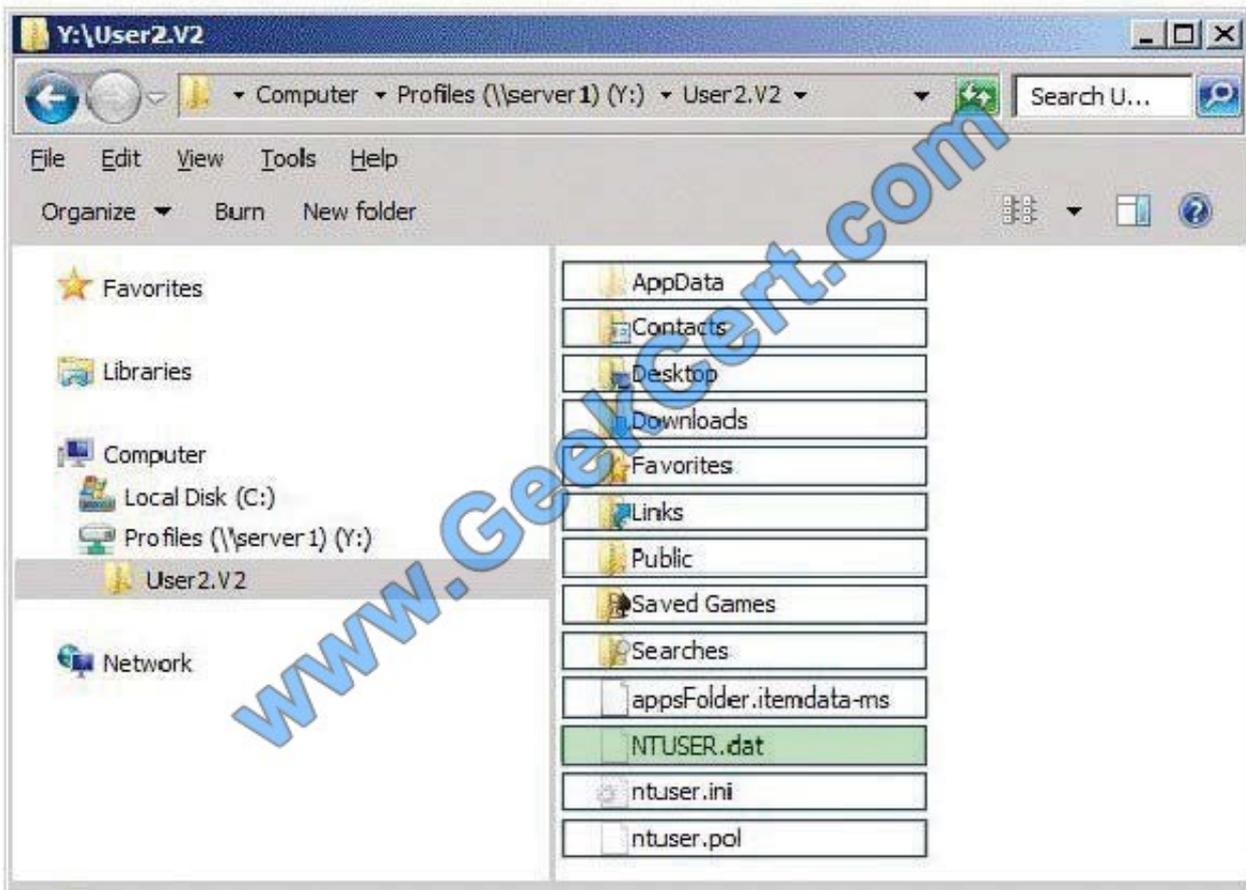
Hot Area:

Answer Area

Correct Answer:

Answer Area

An archive file on client computers that is updated each time the Administrative Templates CSE sets a policy setting. As processing completes, an Ntuser.pol containing the history of applied registry based policies in the Group Policy managed policies tree is written to the root of the user's profile containing user policy settings and to the "all users" profile containing computer policy settings.(%Allusersprofile%\ntuser.pol for computer policy and %userprofile%\ntuser.pol for user policy.)

http://technet.microsoft.com/en-us/library/cc758189%28v=WS.10%29.aspx

The NTUSER.DAT file on a Microsoft Windows computer is a registry file that stores the software and operating system settings for each user profile.

NTUSER.INI is a hidden file in Documents and Settings\ There is one for each user account on the machine. and is used to set up the user roaming profile components.

The ntuser.ini file is used to set up the user roaming profile components that are not copied to the server.

QUESTION 5

You administer Windows 8.1 Enterprise computers that are members of a workgroup.

Company policy requires that all computers receive the latest updates from a Windows Update. Only updates that are digitally signed by Microsoft are installed.

You need to configure the computers to automatically receive and apply the updates.

What should you do first?

A. Configure the Configure Automatic Updates policy setting to Allow local admin to choose setting.

B. Configure the Specify intranet Microsoft update service location policy setting to use the local WSUS server.

C. Enable the Allow signed updates from an intranet Microsoft update service location policy setting.

D. Configure the Configure Automatic Updates policy setting to Auto download and schedule for install.

Correct Answer: D

Explanation: Group Policy setting: Auto download and schedule the install You can specify the schedule by using the options in this Group Policy setting. If no schedule is specified, the default schedule for all installations will be every day at

3:00 A.M. If any updates require a restart to complete the installation, Windows will restart the computer automatically. (If a user is signed in to the computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.)

Reference: Step 5: Configure Group Policy Settings for Automatic Updates https://technet.microsoft.com/en-us/library/dn595129.aspx

Latest 70-688 Dumps   70-688 PDF Dumps   70-688 Exam Questions

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.geekcert.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: