



70-692^{Q&As}

Upgrading Your Windows XP Skills to MCSA Windows 8

Pass Microsoft 70-692 Exam with 100% Guarantee

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

<https://www.lead4pass.com/70-692.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

A company has an Active Directory Domain Services (AD DS) domain. All client computers run Windows 8.1.

You need to configure 20 portable computers so that they sleep after 20 minutes when running on battery power. You must accomplish this goal by using the least amount of administrative effort.

Which two actions should you perform? (Each correct answer presents part of the complete solution. Choose two.)

- A. Edit the local Group Policy to configure the Shut Down options.
- B. Create a Group Policy object (GPO) that configures the Sleep Management settings.
- C. Create a Group Policy object (GPO) that configures the Power Management settings.
- D. Link the Group Policy object (GPO) to the organizational unit containing the portable computers.
- E. Edit the local Group Policy to configure the Power Management settings.

Correct Answer: CD

Explanation: Put the Laptops into an OU.

Create an appropriate GPO.

Link the GPO to the OU.

Note:

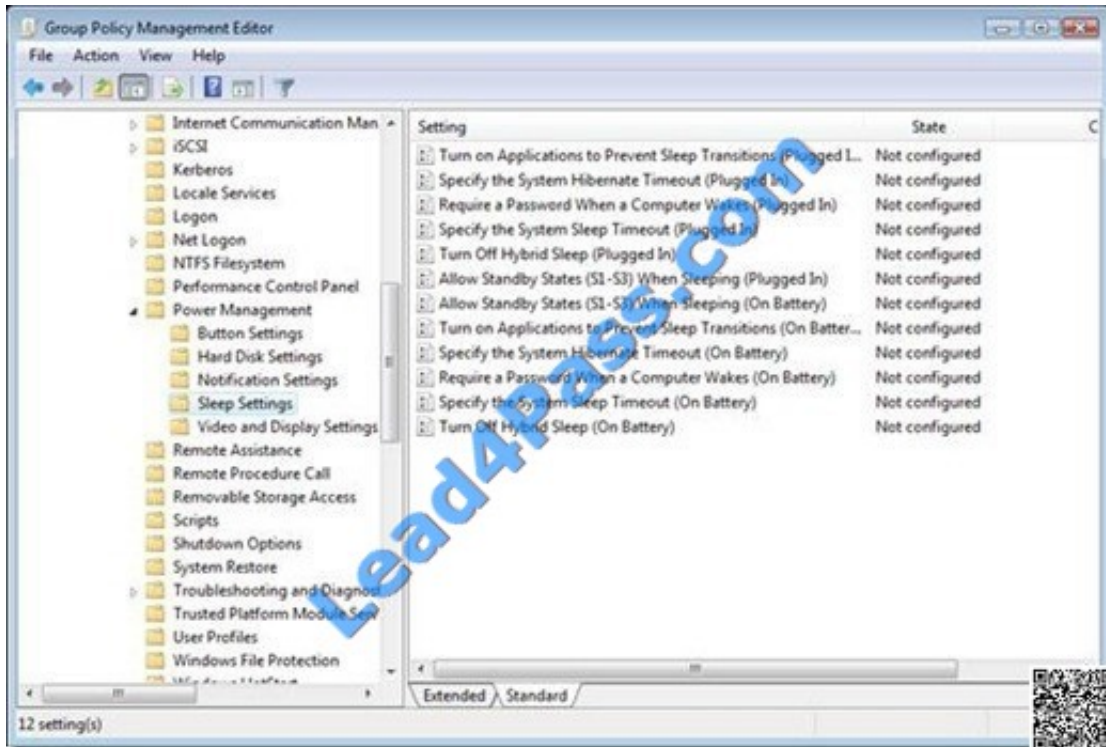
* Networking power management (not sleep management) refers to the set of features that you can configure to allow the computers in your network to save energy.

Incorrect:

Local Group Policy would have to be edited locally on each laptop.

<http://blogs.technet.com/b/askds/archive/2008/03/19/managing-power-with-group-policy-part-2-or-3.aspx>

Managing Power with Group Policy: Part 2 of 3



C:\Users\Chaudhry\Desktop\1.jpg

Another related policy setting is Specify the System Sleep Timeout, only the value entered (in seconds) indicates how much idle time elapses before Windows enters sleep mode.

Further Information:

Put the Laptops into an OU.

Create an appropriate GPO.

Link the GPO to the OU.

QUESTION 2

A company has Windows 8.1 client computers. The company uses Windows BitLocker Drive Encryption and BitLocker Network Unlock on all client computers.

Your need to collect information about BitLocker Network Unlock status.

Which command should you run?

- A. Run the BdeHdCfg command.
- B. Run the bitsadmin command.
- C. Run the BitLockerWizard command.
- D. Run the manage-bde command.



Correct Answer: D

QUESTION 3

You are the system administrator for Contoso, Ltd.

The human resource director's Windows 8.1 computer crashes at login this morning. After powering off and restarting the computer, you successfully boot it, and the human resource director is able to log in. Later in the day, the director

reports that the computer is still not functioning properly. Apps are opening extremely slowly, and the computer locks up for minutes at a time. You have not taken any disaster recovery steps prior to this problem. You decide to recover the

computer's operating system.

You need to ensure that the recovery does not affect the human resource director's current data, personalization settings, and windows store apps.

Which utility should you use?

- A. Reset PC
- B. System Restore
- C. File Recovery
- D. Recovery Drive

Correct Answer: A

QUESTION 4

You are the network administrator for Contoso, Ltd. Many users have Windows 8.1 laptops, and your IT department configures all of them to use BitLocker on all fixed drives.

Many users carry sensitive corporate data on their USB drives.

You need to enable BitLocker for these USB drives.

Which key protector option should you use?

- A. TPM
- B. A .tpmfile
- C. Automatic Unlock
- D. A smartcard

Correct Answer: B

QUESTION 5



A company has an Active Directory Domain Services (AD DS) domain with Windows 8.1 client computers.

You need to minimize the amount of Trusted Platform Module (TPM) authorization information that is stored in the registry.

What should you do?

- A. Create a Group Policy object (GPO) that sets the Configure the level of TPM owner authorization information available to operating system policy setting to None.
- B. Create a Group Policy object (GPO) that enables the Turn on TPM Local Encryption policy setting.
- C. Create a Group Policy object (GPO) that disables the Configure the level of TPM owner authorization information available to operating system policy setting.
- D. Enable Platform Configuration Register indices (PCRs) 0, 2, 4, and 11 for the Configure TPM validation profile for native UEFI firmware configuration policy setting.

Correct Answer: A

Explanation: http://technet.microsoft.com/en-us/library/jj679889.aspx#BKMK_tpmgp_oauthos Configure the level of TPM owner authorization information available to the operating system

This policy setting configures how much of the TPM owner authorization information is stored in the registry of the local computer. Depending on the amount of TPM owner authorization information that is stored locally, the Windows operating

system and TPM- based applications can perform certain actions in the TPM that require TPM owner authorization without requiring the user to enter the TPM owner password.

There are three TPM owner authentication settings that are managed by the Windows operating system.

You can choose a value of Full, Delegate, or None. Full - This setting stores the full TPM owner authorization, the TPM administrative delegation blob, and the TPM user delegation blob in the local registry. With this setting, you can use the

TPM without requiring remote or external storage of the TPM owner authorization value. This setting is appropriate for scenarios that do not require you to reset the TPM anti-hammering logic or change the TPM owner authorization value.

Some TPM- based applications may require that this setting is changed before features that depend on the TPM anti-hammering logic can be used. Delegated - This setting stores only the TPM administrative delegation blob and the TPM

user delegation blob in the local registry. This setting is appropriate for use with TPM-based applications that depend on the TPM antihammering logic. When you use this setting, we recommend using external or remote storage for the full

TPM owner authorization value--for example, backing up the value in Active Directory Domain Services (AD DS).

None - This setting provides compatibility with previous operating systems and applications. You can also use it for scenarios when TPM owner authorization cannot be stored locally. Using this setting might cause issues with some TPM-

based applications.

Further Information:

<http://technet.microsoft.com/en-us/library/cc770660.aspx> Active Directory Domain Services (AD DS) can be used to store Trusted Platform Module (TPM) recovery information.



There is only one TPM owner password per computer; therefore, the hash of the TPM owner password is stored as an attribute of the computer object in AD DS. The attribute has the common name (CN) of ms-TPM-OwnerInformation.
http://

www.group-policy.com/ref/policy/2859/Configure_TPM_platform_validation_profile Configure TPM platform validation profile

This policy setting allows you to configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if

BitLocker has already been turned on with TPM protection.

If you enable this policy setting before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM will not release the encryption key to unlock the drive and the computer will instead display the BitLocker Recovery console and require that either the recovery password or recovery key be provided to unlock the drive.

If you disable or do not configure this policy setting, the TPM uses the default platform validation profile or the platform validation profile specified by the setup script. A platform validation profile consists of a set of Platform Configuration Register (PCR) indices ranging from 0 to 23. The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). The descriptions of PCR settings for computers that use an Extensible Firmware Interface (EFI) are different than the PCR settings described for computers that use a standard BIOS. The BitLocker Drive Encryption Deployment Guide on Microsoft TechNet contains a complete list of PCR settings for both EFI and standard BIOS. Warning: Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion (respectively) of the PCRs.

[70-692 PDF Dumps](#)

[70-692 VCE Dumps](#)

[70-692 Study Guide](#)



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](#)

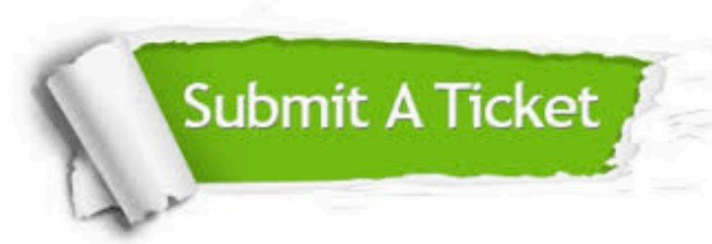
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.lead4pass.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © lead4pass, All Rights Reserved.