

100% Money Back
Guarantee

Vendor:Microsoft

Exam Code:70-744

Exam Name:Securing Windows Server 2016

Version:Demo

QUESTION 1

Your network contains an Active Directory named contoso.com.

The domain contains the computers configured as shown in the following table.

Name	IP address
Server1	172.16.1.30
Computer1	172.16.10.60
Computer2	172.16.20.50

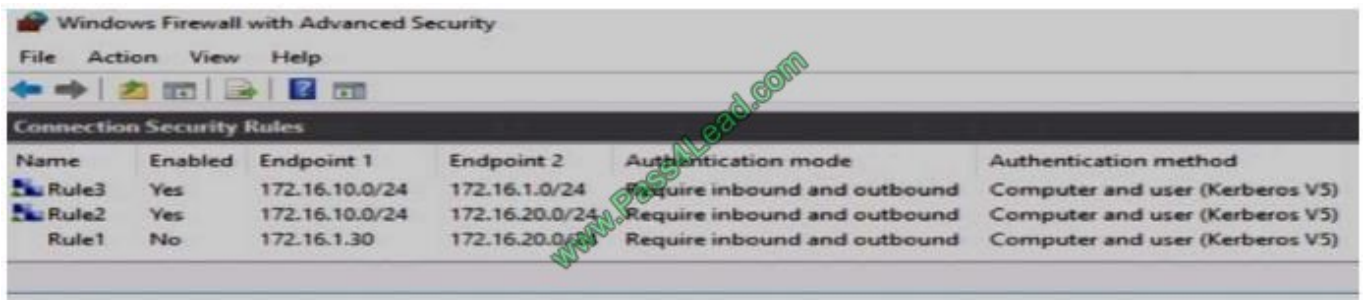
Server1 has a share named Share1 that has the following configurations

```

PresetPathAcl      : System.Security.AccessControl.DirectorySecurity
ShareState         : Online
AvailabilityType   : NonClustered
ShareType          : FileSystemDirectory
FolderEnumerationMode : Unrestricted
CachingMode        : Manual
SmbInstance        : Default
CATimeout          : 0
ConcurrentUserLimit : 0
ContinuouslyAvailable : False
CurrentUsers       : 0
Description        :
EncryptData        : True
Name               : Share1
Path               : C:\Shares\Share1
Scoped             : False
ScopeName          :
SecurityDescriptor : D:BAD:DUD:(A;OICI;FA;;;WD)
ShadowCopy         : False
Special            : False
Temporary          : False

PSComputerName    :
CimClass           : ROOT/Microsoft/Windows/SMB:MSFT_SmbShare
CimInstanceProperties : {AvailabilityType, CachingMode, CATimeout, Conc
CimSystemProperties : Microsoft.Management.Infrastructure.CimSystemPr
```

Server1, Computer1, and Computer2 have the connection security rules configured as shown in follow:



The screenshot shows the Windows Firewall with Advanced Security console. The 'Connection Security Rules' section is expanded, displaying a table of rules. The table has columns for Name, Enabled, Endpoint 1, Endpoint 2, Authentication mode, and Authentication method. Three rules are listed: Rule3, Rule2, and Rule1. Rule3 and Rule2 are enabled, while Rule1 is disabled. All three rules require inbound and outbound authentication and use Computer and user (Kerberos V5) as the authentication method.

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method
Rule3	Yes	172.16.10.0/24	172.16.1.0/24	Require inbound and outbound	Computer and user (Kerberos V5)
Rule2	Yes	172.16.10.0/24	172.16.20.0/24	Require inbound and outbound	Computer and user (Kerberos V5)
Rule1	No	172.16.1.30	172.16.20.0/24	Require inbound and outbound	Computer and user (Kerberos V5)

Please Select the correct statement as below:

Hot Area:

Statements	Yes	No
When Computer1 accesses Share1. SMB encryption will be used.	<input type="radio"/>	<input type="radio"/>
When Computer2 accesses Share1. IPsec encryption will be used	<input type="radio"/>	<input type="radio"/>
When Server1 access a shared folder on Computer1. IPsec encryption will be used.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
When Computer1 accesses Share1. SMB encryption will be used.	<input checked="" type="radio"/>	<input type="radio"/>
When Computer2 accesses Share1. IPsec encryption will be used	<input checked="" type="radio"/>	<input type="radio"/>
When Server1 access a shared folder on Computer1. IPsec encryption will be used.	<input type="radio"/>	<input checked="" type="radio"/>

When Computer1 accesses Share1, SMB encryption will be used: YES When Computer2 accesses Share1, SMB encryption will be used: YES When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: NO The shared folder "Share1" is configured with "EncryptData : True", no matter which network the client resides, SMB 3 communication will be encrypted. When Server1 access Computer1 over network, the original packet L3 IP Header is as

follow:-172.16.1.30 ?gt; 172.16.10.60 These traffic does not match the enabled IPsec rule "Rule2" nor "Rule3", and the only matching rule "Rule1" is disabled. So, no IPsec encryption will be achieved.

QUESTION 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016. All client computers run Windows 10.

The relevant objects in the domain are configured as shown in the following table.

Server name	Object	Organizational unit (OU) name
Server1	Computer account	Servers
Server2	Computer account	Servers
User1	User account	Operations Users

You need to assign User1 the right to restore files and folders on Server1 and Server2.

Solution: You add User1 to the Backup Operators group in contoso.com.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

References:

[https://technet.microsoft.com/en-us/library/cc771990\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771990(v=ws.11).aspx)

users. The solution would let User1 to backup files and folders on domain controllers for contoso.com instead.

QUESTION 3

Your network contains an Active Directory forest named contoso.com. The functional level of the forest and the domain is Windows Server 2012 R2.

You plan to use Local Administrator Password Solution (LAPS) for all member servers.

You need to prepare the forest for LAPS.

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

NOTE: Each correct selection is worth one point.

A. Run the Set-AdmPwdComputerSelfPermission cmdlet.

B. Install the LAPS client-side extension on all domain controllers.

C. Run the Update-AdmPwdADSchema cmdlet.

D. Run the Set-AdmPwdAuditing cmdlet.

E. Deploy an enterprise certification authority (CA).

Correct Answer: AC

<https://blog.thesysadmins.co.uk/deploying-microsoft-laps-part-1.html>

QUESTION 4

The New-CIPolicy cmdlet creates a Code Integrity policy as an .xml file. If you do NOT supply either driver files or rules what will happen?

- A. The cmdlet performs a system scan
- B. An exception/warning is shown because either one is required
- C. Nothing
- D. The cmdlet searches the Code Integrity Audit log for drivers

Correct Answer: A

If you do not supply either driver files or rules, this cmdlet performs a system scan similar to the Get-SystemDriver cmdlet. The cmdlet generates rules based on Level. If you specify the Audit parameter, this cmdlet scans the Code Integrity Audit log instead.

QUESTION 5

Your network contains an Active Directory domain named contoso.com. The domain contains several shielded virtual machines.

You deploy a new server named Server1 that runs Windows Server 2016. You install the Hyper-V server role on Server1.

You need to ensure that you can host shielded virtual machines on Server1.

What should you install on Server1?

- A. Host Guardian Hyper-V Support
- B. BitLocker Network Unlock
- C. the Windows Biometric Framework (WBF)
- D. VM Shielding Tools for Fabric Management

Correct Answer: A

This question mentions "The domain contains several shielded virtual machines.", which indicates a working Host Guardian Service deployment was completed. <https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabricshielded-vm/guarded-fabricguarded-host-prerequisites> For a new Hyper-V server to utilize an existing Host Guardian Service, install the "Host Guardian Hyper-V Support".

Guarded hosts using TPM mode must meet the following prerequisites:

- **Hardware:** One host is required for initial deployment. To test Hyper-V live migration for shielded VMs, you must have at least two hosts.

Hosts must have:

- IOMMU and Second Level Address Translation (SLAT)
- TPM 2.0
- UEFI 2.3.1 or later
- Configured to boot using UEFI (not BIOS or "legacy" mode)
- Secure boot enabled

- **Operating system:** Windows Server 2016 Datacenter edition

Important

Make sure you install the latest cumulative update.

- **Role and features:** Hyper-V role and the Host Guardian Hyper-V Support feature. The Host Guardian Hyper-V Support feature is only available on Datacenter editions of Windows Server 2016.

QUESTION 6

Your network contains an Active Directory domain named contoso.com.

The domain contains four global groups named Group1, Group2, Group3, and Group4. A user named User1 is a member of Group3.

You have an organizational unit (OU) named OU1 that contains computer accounts. A Group Policy object (GPO) named GPO1 is linked to OU1. OU1 contains a computer account named Computer1.

GPO1 has the User Rights Assignment configured as shown in the following table.

- A. Modify the membership of Group3.
- B. Modify the membership of Group2.
- C. Modify the membership of Group1.
- D. Modify the membership of Group4.

Correct Answer: B

QUESTION 7

You have a server named Server1 that runs Windows Server 2016. You need to identify whether any connection security rules are configured on Server1. Which cmdlet should you use?

- A. Get-NetIPSecRule
- B. Get-NetFirewallRule
- C. Get-NetFirewallProfile

- D. Get-NetFirewallSetting
- E. Get-NetFirewallPortFilter
- F. Get-NetFirewallAddressFilter
- G. Get-NetFirewallSecurityFilter
- H. Get-NetFirewallApplicationFilter

Correct Answer: A

<https://technet.microsoft.com/en-us/itpro/powershell/windows/netsecurity/get-netipsecrule> Get-NetIPSecRule displays the existence and details of Connection Security Rules, as connection securityrules implements IPsec between computers (not usingtunnel endpoints) or sites (using tunnel endpoints)

QUESTION 8

You are creating a Nano Server image for the deployment of 10 servers.

You need to configure the servers as guarded hosts that use Trusted Platform Module (TPM) attestation.

Which three packages should you include in the Nano Server image? Each correct answer presents part of the solution.

- A. Microsoft-NanoServer-SecureStartup-Package
- B. Microsoft-NanoServer-ShieldedVM-Package
- C. Microsoft-NanoServer-Storage-Package
- D. Microsoft-NanoServer-SCVMM-Compute-Package
- E. Microsoft-NanoServer-SCVMM-Package
- F. Microsoft-NanoServer-Compute-Package

Correct Answer: ABF

<https://docs.microsoft.com/en-us/system-center/vmm/guarded-deploy-host?toc=/windows-server/virtualization/toc.json>For an SCVMM Managed Nano Server Hyper-V case:If your host is running Nano Server Hyper-V host, it should have the Compute, SCVMM-Package, SCVMMCompute, SecureStartup, and ShieldedVM packagesinstalled.<https://docs.microsoft.com/en-us/windows-server/get-started/deploy-nano-server>For an standalone Nano Server Hyper-V host, no SCVMM related packages are required, only Compute, SecureStartup, and ShieldedVM packages are required.This table shows the roles and features that are available in this release of Nano Server, along with theWindows PowerShell options that will install the packagesfor them.Some packages are installed directly with their own Windows PowerShell switches (such as -Compute); othersyou install by passing package names to the ackage parameter, which you can combine in a comma-separated list. You can dynamically list availablepackages using the Get-NanoServerPackage cmdlet.

Role or feature	Option
Hyper-V role (including NetQoS)	-Compute
Failover Clustering and other components, detailed after this table	-Clustering
Basic drivers for a variety of network adapters and storage controllers. This is the same set of drivers included in a Server Core installation of Windows Server 2016.	-OEMDrivers
File Server role and other storage components, detailed after this table	-Storage
Windows Defender, including a default signature file	-Defender
Reverse forwarders for application compatibility, for example common application frameworks such as Ruby, Node.js, etc.	Now included by default
DNS Server role	-Package Microsoft-NanoServer-DNS-Package
PowerShell Desired State Configuration (DSC)	-Package Microsoft-NanoServer-DSC-Package Note: For full details, see Using DSC on Nano Server.
Internet Information Server (IIS)	-Package Microsoft-NanoServer-IIS-Package Note: See IIS on Nano Server for details about working with IIS.
Host support for Windows Containers	-Containers
System Center Virtual Machine Manager agent	-Package Microsoft-NanoServer-SCVMM-Package -Package Microsoft-NanoServer-SCVMM-Compute-Package Note: Use the SCVMM Compute package only if you are monitoring Hyper-V. For hyper-converged deployments in VMM, you should also specify the -Storage parameter. For more details, see the VMM documentation.
System Center Operations Manager agent	Installed separately. See the System Center Operations Manager documentation for more details at https://technet.microsoft.com/en-us/system-center-docs/om/manage/install-agent-on-nano-server .
Data Center Bridging (including DCBQoS)	-Package Microsoft-NanoServer-DCB-Package
Deploying on a virtual machine	-Package Microsoft-NanoServer-Guest-Package
Deploying on a physical machine	-Package Microsoft-NanoServer-Host-Package
BitLocker, trusted platform module (TPM) volume encryption, platform identification, cryptography providers, and other functionality related to secure startup	-Package Microsoft-NanoServer-SecureStartup-Package
Hyper-V support for Shielded VMs	-Package Microsoft-NanoServer-ShieldedVM-Package Note: This package is only available for the Datacenter edition of Nano Server.

QUESTION 9

Name	Operating system
Computer1	Windows 8.1
Computer2	Windows 10
Server1	Windows Server 2016
Server2	Windows Server 2016

Your network contains an Active Directory domain. The domain contains the computers shown in the following table.

Server 1 is a file server that has two shared folders named Share1 and Share2. Share1 has encryption enabled. Share2 has encryption disabled. Domain users have read access to both shares.

From PowerShell, you run `set-smbServerConfiguration -EncryptData $true -Force`.

For each of the following statements select Yes if the statement is true. Otherwise, Select No.

Hot Area:

	Yes	No
If you connect to Share1 from Server2, network traffic will be encrypted	<input type="radio"/>	<input type="radio"/>
If a user attempts to connect to Share1 from Computer1, the user will be prevented from accessing Share1	<input type="radio"/>	<input type="radio"/>
If you connect to Share2 from Computer2, network traffic will be encrypted	<input type="radio"/>	<input type="radio"/>

Correct Answer:

	Yes	No
If you connect to Share1 from Server2, network traffic will be encrypted	<input checked="" type="radio"/>	<input type="radio"/>
If a user attempts to connect to Share1 from Computer1, the user will be prevented from accessing Share1	<input type="radio"/>	<input checked="" type="radio"/>
If you connect to Share2 from Computer2, network traffic will be encrypted	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 10

Your data center contains 10 Hyper-V hosts that host 100 virtual machines.

You plan to secure access to the virtual machines by using the Datacenter Firewall service.

You have four servers available for the Datacenter Firewall service. The servers are configured as shown in the following table.

Server name	Platform	Windows Server 2016 edition
Server20	Physical	Standard
Server21	Physical	Standard
Server22	Virtual	Datacenter
Server23	Virtual	Datacenter

You need to install the required server roles for the planned deployment

Which server role should you deploy? Choose Two.

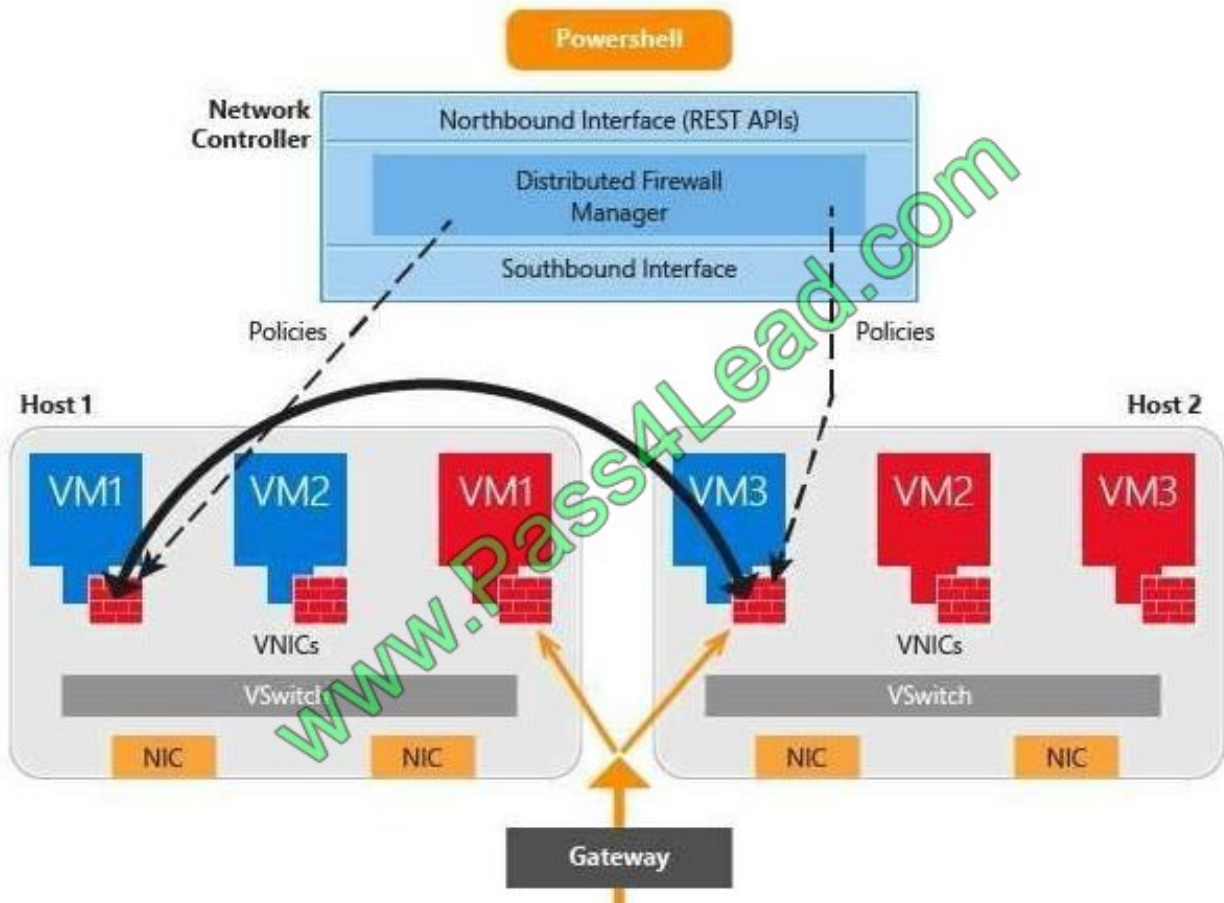
- A. Server role to deploy: Multipoint Services
- B. Server role to deploy: Network Controller
- C. Server role to deploy: Network Policy and Access Services
- D. Servers on which to deploy the server role: Server20 and Server21
- E. Servers on which to deploy the server role: Server22 and Server23

Correct Answer: BE

Datacenter Firewall is a new service included with Windows Server 2016. It is a network layer, 5-tuple (protocol, source and destination port numbers, source and destination IP addresses), stateful, multitenant firewall. When deployed and offered as a service by the service provider, tenant administrators can install and configure firewall policies to help protect their virtual networks from unwanted traffic originating from Internet and intranet networks.

<https://docs.microsoft.com/en-us/windows-server/networking/sdn/technologies/network-controller/network-controller>
 Network Controller Features The following Network Controller features allow you to configure and manage virtual and physical network devices and services. i) Firewall Management (Datacenter Firewall) ii) Software Load Balancer Management iii) Virtual Network Management iv) RAS Gateway Management <https://docs.microsoft.com/en-us/windows-server/networking/sdn/plan/installation-and-preparation-requirements-for-deploying-network-controller> Installation

requirements Following are the installation requirements for Network Controller. For Windows Server 2016 deployments, you can deploy Network Controller on one or more computers, one or more VMs, or a combination of computers and VMs. All VMs and computers planned as Network Controller nodes must be running Windows Server 2016 Datacenter edition.



QUESTION 11

Your network contains an Active Directory domain named contoso.com. All client computers run Windows 10.

You plan to deploy a Remote Desktop connection solution for the client computers.

You have four available servers in the domain that can be configured as Remote Desktop servers. The servers are configured as shown in the following table.

Server name	Operating system	Location
Server1	Windows Server 2012 R2	on-premises
Server2	Windows Server 2016	Microsoft Azure
Server3	Windows Server 2016	on-premises
Server4	Windows Server 2012 R2	Microsoft Azure

You need to ensure that all Remote Desktop connections can be protected by using Remote Credential Guard.

Solution: You deploy the Remote Desktop connection solution by using Server4.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

No, as Server4 is a Windows Server 2012R2 which does not meet the requirements of Remote Credential Guard.
<https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard>
Remote Credential Guard requirements
To use Windows Defender Remote Credential Guard, the Remote Desktop client and remote host must meet the following requirements:
The Remote Desktop client device:
Must be running at least Windows 10, version 1703 to be able to supply credentials.
Must be running at least Windows 10, version 1607 or Windows Server 2016 to use the user's signed-in credentials. This requires the user's account be able to sign in to both the client device and the remote host.
Must be running the Remote Desktop Classic Windows application. The Remote Desktop Universal Windows Platform application doesn't support Windows Defender Remote Credential Guard.
Must use Kerberos authentication to connect to the remote host. If the client cannot connect to a domain controller, then RDP attempts to fall back to NTLM. Windows Defender Remote Credential Guard does not allow NTLM fallback because this would expose credentials to risk.
The Remote Desktop remote host:
Must be running at least Windows 10, version 1607 or Windows Server 2016.
Must allow Restricted Admin connections.
Must allow the client's domain user to access Remote Desktop connections.
Must allow delegation of non-exportable credentials.

QUESTION 12

Your network contains an Active Directory domain named contoso.com. The domain contains 100 servers.

You deploy the Local Administrator Password Solution (LAPS) to the network.

You discover that the members of a group named FinanceAdministrators can view the password of the local Administrator accounts on the servers in an organizational unit (OU) named FinanceServers.

You need to prevent the FinanceAdministrators members from viewing the local administrators' passwords on the servers in FinanceServers. Which permission should you remove from FinanceAdministrators?

- A. all extended rights
- B. read all properties
- C. read permissions
- D. list contents

Correct Answer: A

<https://4sysops.com/archives/set-up-microsoft-laps-local-administrator-password-solution-in-active-directory/>

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

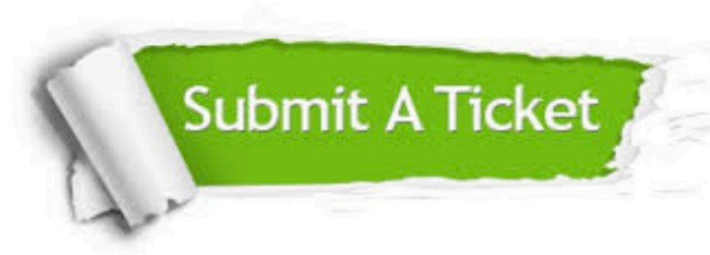
More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

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.