Guidance

End User Devices Security Guidance: Windows 7

Updated 11 November 2014

Contents

This guidance is applicable to devices running Enterprise versions of Windows 7 SP1, acting as client operating systems, which include BitLocker Drive Encryption, AppLocker and Windows VPN features.

This guidance was developed following testing performed on a Windows Hardware Certified ⬈ device running Windows 7 Enterprise SP1.

1. Changes since previous guidance

This document updates the previous guidance to cover Windows 7 with Service Pack 1.

Changes to the recommended configuration have been made to take account of the CPA certification ⬈ for Microsoft's IPsec client as well as updates to the Microsoft Security Baselines. The risk information given below has been updated to reflect these changes.

Deployments which followed the previous recommended configuration will need to replace the previous group policy (including EMET settings) with the new configuration.

2. Usage scenario

Windows 7 SP1 devices will be used remotely over any network bearer, including Ethernet, Wi-Fi and 3G, to connect back to the enterprise over a VPN. This enables a variety of remote working approaches such as:

- accessing OFFICIAL email

- creating, editing, reviewing and commenting on OFFICIAL documents

- accessing the OFFICIAL intranet resources, the Internet and other web resources

To support these scenarios, the following architectural choices are recommended:

- all data should be routed over a secure enterprise VPN to ensure the Confidentiality and Integrity of the traffic, and to benefit from enterprise protective monitoring solutions

- arbitrary third party application installation by users is not permitted on the device. Applications should be authorised by an administrator and deployed via a trusted mechanism

- most users should use accounts with no administrative privileges. Users that require administrative privileges should use a separate unprivileged account for email and web browsing. It is recommended that local administrator accounts have a unique strong password per device

3. Summary of platform security

This platform has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	
2. Assured data-at-rest protection	
3. Authentication	

4. Secure boot	Secure boot is not supported on this platform.
5. Platform integrity and application sandboxing	
6. Application whitelisting	Application Whitelisting is fully supported on this platform when Microsoft KB2532445 has been applied
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	
10. Device update policy	
11. Event collection for enterprise analysis	
12. Incident response	

4. How the platform can best satisfy the security recommendations

This section details the platform security mechanisms which best address each of the security recommendations.

4.1 Assured data-in-transit protection

Use DirectAccess ⬈ or the native IKEv2 IPsec VPN configured as per the Windows VPN Security Procedures.

If using DirectAccess use the CPA customisation guide (available via CESG enquiries) to configure the client.

If using the native IKEv2 IPsec VPN use the Windows Firewall to block outbound connections when the VPN is not active. The L2TP and IPsec VPNs do not initiate automatically at boot and there is potential for the user to disconnect the VPN at any time. An example firewall profile is provided in the Configuration Settings section which demonstrates how to mitigate this behaviour.

Alternatively the Windows 7 platform allows the use of third party VPN clients. Use a correctly configured CPA Foundation grade client.

4.2   Assured data-at-rest protection

Use one of the following configurations to provide full volume encryption:

- BitLocker with a TPM and 7 character complex Enhanced PIN configured in alignment with the [BitLocker configuration settings](#)

- An independently assured CPA Foundation Grade Data at Rest encryption product configured in alignment with the security procedures for that product

If deploying BitLocker, allow the software to generate all key material required (no CESG entropy or key material is required). Deploy the [BitLocker configuration settings](#) before encryption is started.

BitLocker is not Foundation Grade certified. However, CESG has determined that the level of protection it provides is equivalent to Foundation Grade when configured as per this guidance.

4.3   Authentication

The user implicitly authenticates to the device by decrypting the disk at boot time.

The user then has a secondary strong 9 character password to authenticate them to the platform at boot and unlock time. This password also derives a key which encrypts certificates and other credentials, giving access to enterprise services.

After logon, the credentials will be best protected if the user is a member of the Protected Users group on the domain and LSASS is marked as a [Protected Process](#).

End User Devices used to perform administrative functions should take advantage of the [Restricted Admin](#) feature of Remote Desktop Connections. User accounts with administrative privileges should use a strong 14 character secondary password to authenticate them to the platform at logon and unlock time. The credentials will be best protected if the administrative user is a member of the Protected Users group on the domain, and have [Authentication Policy Silos](#) applied.

4.4   Secure boot

A UEFI/BIOS password can make it more difficult for an attacker to modify the boot process. With physical access, the boot process can still be compromised.

4.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

4.6 Application whitelisting

An enterprise configuration can be applied to implement application control (using AppLocker). A recommended sample configuration that only allows Administrator-installed applications to run is provided below.

In addition Microsoft HotFixes KB977542 and KB2532445 should also be installed to enhance the AppLocker protection mechanisms.

4.7 Malicious code detection and prevention

Windows 7 SP1 includes Windows Defender ⬀ that attempts to detect malicious code for this platform. Alternatively, several third party anti-malware products are available.

The Microsoft Enhanced Mitigation Experience Toolkit ⬀ (EMET) should be used to help prevent vulnerabilities in software from being successfully exploited.

4.8 Security policy enforcement

Settings applied through Group Policy cannot be modified by unprivileged users.

4.9 External interface protection

Interfaces can be configured using group policy. USB removable media can be blocked through Group Policy if required. Direct Memory Access (DMA) is possible from peripherals connected to some external interfaces including FireWire, eSATA, and Thunderbolt unless disabled through group policy as detailed below or in the UEFI/BIOS.

4.10 Device update policy

Windows Server Update Service (WSUS) is used to enforce updates of the core platform and any Windows applications. This can also be used to update third party applications.

## 4.11 Event collection for enterprise analysis

Event collection can be carried out using Windows Event Forwarding for central event log collection.

4.12 Incident response

The combination of BitLocker drive encryption and enterprise revocation of user credentials are appropriate for managing this security recommendation.

5. Network architecture

All remote or mobile working scenarios should use a typical remote access architecture based on the Walled Garden Architectural Pattern. The following network diagram describes the recommended architecture for this platform.
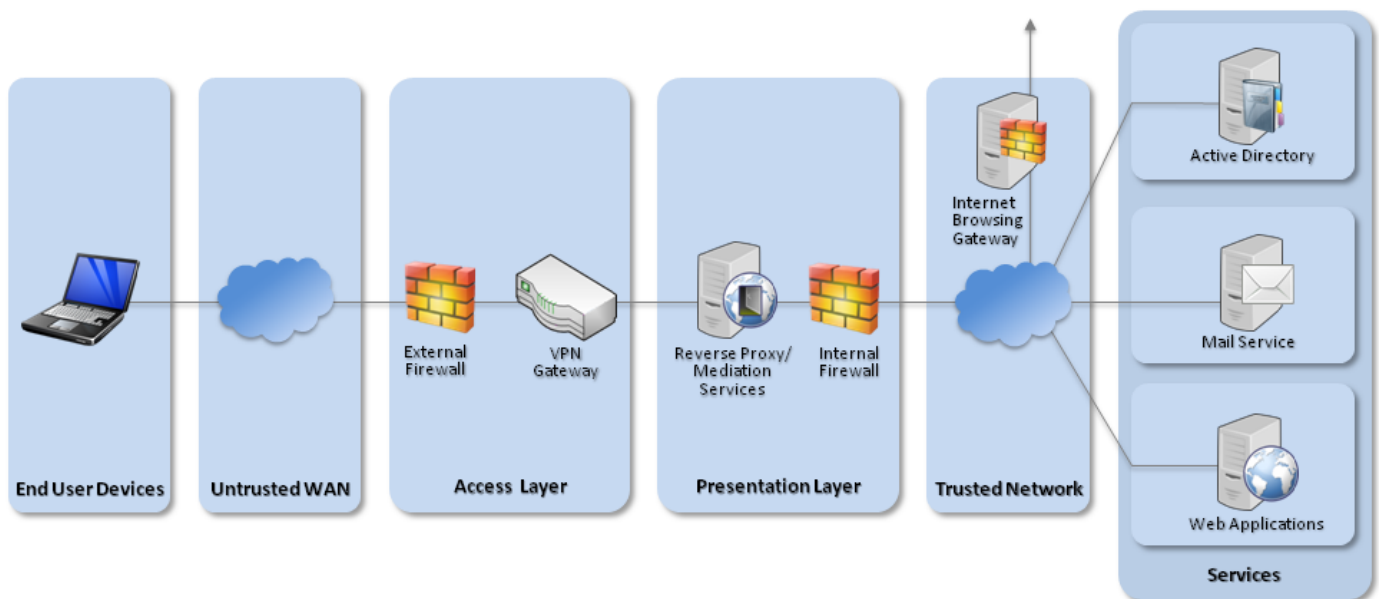
Recommended network architecture for Windows 7 deployments

6. Deployment process

The steps below should be followed to prepare the enterprise infrastructure for hosting a deployment of these devices:

1. Procure, deploy and configure network components, including an approved IPsec VPN Gateway.

2. Configure Windows Server Update Services (WSUS) following [Microsoft's deployment guidance ⬈](#).

3. Create Group Policies for user and computer groups in accordance with the settings later in this section ensuring that the Microsoft Baseline settings have the lowest precedence when being deployed.

4. Deploy an AppLocker rule set using Group Policy following guidance in [Application Whitelisting](#). A sample configuration that only allows applications that have been installed by an Administrator to run is outlined in the [Group Policy settings](#) below.

5. Create Event Forwarding Subscriptions and configure Group Policy to forward at least AppLocker,Application, System and Security logs that have a level of Critical Error or Warning to an event management system as per [NSA guidance ⬈](#).

6. Configure user groups according to the principle of least privilege.

7. Provisioning steps

The steps below should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users:

1. Configure the UEIF/BIOS to disable unused hardware interfaces, check the boot order to prioritise internal storage and set a password to prevent changes.

2. Deploy the most recent version of [EMET ⬈](#) (5.1 at the time of writing) and configure it using [Group Policy configuration](#) given below.

8. Configuration settings

In addition to the following standard Microsoft baselines that are distributed via the [SCM tool ⬈](#), the listed configurations below should be applied through Group Policy Management:

- MSFT Windows 7 SP1 Computer Security Compliance 1.0

- MSFT Windows 7 SP1 User Security Compliance 1.0

- MSFT Internet Explorer 11 Baseline 1.0

Microsoft have published [Additional information 🖅](#) discussing the changes in the baselines for Internet Explorer 11.

For easy configuration, you can download a [zip file containing the custom CESG GPO settings 🖅](#).

The Microsoft baseline configuration settings should be configured within Group Policy Management to have the lowest precedence.

8.1 User configuration

Group Policy	Value(s)
User Configuration > Policies > Administrative Templates > Control Panel > Personalization > Screen saver timeout	300
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Disable changing Automatic Configuration settings	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Do not allow users to enable or disable add-ons	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Prevent "Fix settings" functionality	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Prevent managing SmartScreen Filter	Enabled Select SmartScreen Filter Mode: On
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Disable the Privacy Page	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Disable the Security page	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page > Do not allow resetting Internet Explorer Settings	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page > Turn off encryption support	Enabled Secure Protocol combinations: Use SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Turn on certificate address mismatch warning	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > [All Zones] > Allow font downloads	Disabled

User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > [All Zones] > Scripting of Java applets	Disabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > [All Zones] > Turn on Cross-Site Scripting (XSS) Filter	Enabled Turn on Cross-Site Scripting (XSS) Filter: Enable
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > [All Zones] > Turn on SmartScreen Filter scan	Enabled Use SmartScreen Filter: Enable
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Privacy > Establish Tracking Protection Threshold	Enabled Threshold: 3
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Security Features > Do not display the reveal password button	Enabled
User Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Toolbars > Turn off Developer Tools	Enabled

Group Policy can be used to limit user access to removable media such as USB mass storage devices if required by organisational policy. The settings can be found in `Computer Configuration > Policies > Administrative Templates > System > Removable Storage Access`.

Group Policy can also be used to fully whitelist all devices or device classes which are allowed to be installed. This could be used to allow, for example, basic peripherals such as mice, keyboards, monitors and network cards, but not allow other devices to be connected and installed. It is important to whitelist enough classes of device to allow a successful boot on a variety of hardware.

Details on how to enable whitelisting of specific devices can be found on MSDN ↗.

8.2 Computer configuration

Group Policy	Value(s)
Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Require domain users to elevate when setting a network's location	Enabled
Computer Configuration > Policies > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of devices that match these device IDs	Enabled PCI\CC_0C0A

	d48179be-ec20-11d1-b6b8-00c04fa372a7
	Also apply to matching devices that are already installed: Disabled
Computer Configuration > Policies > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of drivers matching these device setup classes	Enabled
	d48179be-ec20-11d1-b6b8-00c04fa372a7
	Also apply to matching devices that are already installed: Disabled
Computer Configuration > Policies > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon	Enabled
Computer Configuration > Policies > Administrative Templates > System > Power Management > Sleep Settings > Allow standby states (S1-S3) when sleeping (on battery)	Disabled
Computer Configuration > Policies > Administrative Templates > System > Power Management > Sleep Settings > Allow standby states (S1-S3) when sleeping (plugged in)	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > AutoPlay Policies > Disallow Autoplay for non-volume devices	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > AutoPlay Policies > Turn off Autoplay	Enabled
	Turn off Autoplay on: All Drives
Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Security Zones: Use only machine settings	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Tablet PC > Input Panel > Turn off password security in Input Panel	Enabled
	Turn off password security in Input Panel: High
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender > MAPS > Join Microsoft MAPS	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender > Turn off Windows Defender	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Defender > Scan > Check for the latest virus and spyware definitions before running a scheduled scan	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Error Reporting > Disable Windows Error Reporting	Enabled
CN=System > CN=Password Settings Container > CN=Granular Password Settings Users	Precedence: 2
	Enforce minimum password length: 9 characters

	Enforce password history: 8
	Password must meet complexity requirements: Enabled
	Enforce maximum password age: 90 days
	Enforce lockout policy: 5 attempts
	Account will be locked out: Until an administrator manually unlocks the account
	Directly Applies To: Domain Users
CN=System > CN=Password Settings Container > CN=Granular Password Settings Administrators	Precedence: 1
	Enforce minimum password length: 14 characters
	Enforce password history: 24
	Password must meet complexity requirements: Enabled
	Enforce maximum password age: 42 days
	Enforce lockout policy: 5 attempts
	Account will be locked out: Until an administrator manually unlocks the account
	Directly Applies To: Domain Admins
	Protect from accidental deletion: Enabled

8.3 Firewall configuration

Where TCP/UDP ports are specified they refer to the `Remote Port` configuration under `Ports and Protocols` for that rule.

Group Policy	Value(s)

Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Domain Profile	Firewall State : On (Recommended) Inbound connections : Block (default) Outbound connections : Allow (default)
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Domain Profile > Settings > Customize > Apply local firewall rules	No
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Private Profile	Firewall State : On (Recommended) Inbound connections : Block (default) Outbound connections : Block
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Private Profile > Settings > Customize > Apply local firewall rules	No
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Public Profile	Firewall State : On (Recommended) Inbound connections : Block (default) Outbound connections : Block
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Public Profile > Settings > Customize > Apply local firewall rules	No
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Outbound Rules	Enabled General > Action: Allow the connection Programs and Services > Programs > This Program > %SystemRoot%\system32\svchost.exe Advanced > Profiles: Private, Public Allow DHCP (UDP 67/68) Allow DNS (TCP/UDP 53) General > Action: Allow the connection Programs and Services > Programs > This Program > %SystemRoot%\system32\lsass.exe Advanced > Profiles: Private, Public Allow Kerberos (TCP/UDP All Ports) General > Action: Allow the connection Programs and Services > Programs > All Programs that meet the specified conditions Allow LDAP (TCP/UDP 389)

8.4 AppLocker configuration

This example set of rules implements the principle outlined in Enterprise Considerations below. It will not be necessary to customise these rules for most enterprise deployments if using software that adheres to the requirements of Microsoft's Desktop App Certification Program ⬚.

If the rules do need to be customised, follow Microsoft's Design Guide ⬚ to minimise the impact to the operation of the enterprise.

Group Policy	Value(s)
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Executable Rules	Configured: True Enforce Rules
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules	Allow Everyone: All files located in the Program Files folder Allow Everyone: All files located in the Windows folder Exception: %SYSTEM32%\catroot2* Exception: %SYSTEM32%\com* Exception: %SYSTEM32%\com\dmp* Exception: %SYSTEM32%\FxsTmp* Exception: %SYSTEM32%\powershell* Exception: %SYSTEM32%\Spool* Exception: %SYSTEM32%\Tasks* Exception: %SYSTEM32%\Tasks\Microsoft\Windows* Exception: %SYSTEM32%\Tasks\Microsoft\Windows\WCM* Exception: %WINDIR%\debug* Exception: %WINDIR%\debug\wia* Exception: %WINDIR%\pchealth* Exception: %WINDIR%\registration*

	Exception: %WINDIR%\tasks*
	Exception: %WINDIR%\temp*
	Exception: %WINDIR%\tracing*
	Exception: cscript.exe 5.8.0.0-* from Microsoft Corporation
	Exception: wscript.exe 5.8.0.0-* from Microsoft Corporation
	Exception: cmd.exe 6.2.0.0-* from Microsoft Corporation
	Exception: ftp.exe 6.2.0.0-* from Microsoft Corporation
	Exception: net.exe 6.2.0.0-* from Microsoft Corporation
	Exception: net1.exe 6.2.0.0-* from Microsoft Corporation
	Exception: netsh.exe 6.2.0.0-* from Microsoft Corporation
	Exception: powershell.exe 6.2.0.0-* from Microsoft Corporation
	Exception: powershell_ise.exe 6.2.0.0-* from Microsoft Corporation
	Exception: reg.exe 6.2.0.0-* from Microsoft Corporation
	Exception: regedit.exe 6.2.0.0-* from Microsoft Corporation
	Exception: regedt32.exe 6.2.0.0-* from Microsoft Corporation
	Exception: regini.exe 6.2.0.0-* from Microsoft Corporation
	Allow Administrators: All files
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Windows Installer Rules	Configured: True Enforce Rules
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Windows Installer Rules	Allow Administrators: All Windows Installer files
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker >	Configured: True Enforce Rules

Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Script Rules > Enforce rules of this type	Allow Administrators: All Scripts
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > DLL Rules	Configured: True Enforce Rules
Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > DLL Rules	Allow Everyone: All DLLs located in the Program Files folder
	Allow Everyone: All DLLs located in the Windows folder
	Exception: %SYSTEM32%\catroot2*
	Exception: %SYSTEM32%\com*
	Exception: %SYSTEM32%\com\dmp*
	Exception: %SYSTEM32%\FxsTmp*
	Exception: %SYSTEM32%\powershell*
	Exception: %SYSTEM32%\Spool*
	Exception: %SYSTEM32%\Tasks*
	Exception: %SYSTEM32%\Tasks\Microsoft\Windows*
	Exception: %SYSTEM32%\Tasks\Microsoft\Windows\WCM*
	Exception: %WINDIR%\debug*
	Exception: %WINDIR%\debug\wia*
	Exception: %WINDIR%\pchealth*
	Exception: %WINDIR%\registration*
	Exception: %WINDIR%\tasks*
	Exception: %WINDIR%\temp*
	Exception: %WINDIR%\tracing*
	Allow Administrators: All DLLs

8.5 BitLocker configuration

Group Policy	Value(s)
Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Allow enhanced PINs for startup	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Configure minimum PIN length for startup	Enabled Minimum Characters:7
Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Enforce drive encryption type on operating system drives	Enabled Select the encryption type: Full encryption
Computer Configuration > Policies > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication at startup	Enabled Allow BitLocker without a compatible TPM (Requires a password or startup key on a USB flash drive): Unticked Configure TPM startup: Do not allow TPM Configure TPM startup PIN: Allow startup PIN with TPM Configure TPM startup key: Do not allow startup key with TPM Confgure TPM startup key and PIN: Allow startup key and PIN with TPM

8.6 EMET configuration

Group Policy	Value(s)
Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > Default Action and Mitigation Settings	Enabled Deep Hooks: Enabled Anti Detours: Enabled Banned Functions: Enabled Exploit Action: Stop Program
Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > Default Protections for Internet Explorer	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components >	Enabled

Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > Default Protections for Recommended Software	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > System ASLR	Enabled ASRL Setting: Application Opt-In
Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > System DEP	Enabled DEP Setting: Always On
Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > System SEHOP	Enabled SEHOP Setting: Application Opt-Out

Group Policy should be used to apply EMET to Enterprise applications which render untrusted data such as those which are Internet facing. The required settings can be found in `Computer Configuration > Policies > Administrative Templates > Windows Components > EMET > Application Configuration`.

8.7 VPN configuration

If using the native IKEv2 IPsec VPN client, it should be configured to negotiate the following parameters.

Settings	Value(s)
IKE DH Group	14 (2048-bit)
IKE Encryption Algorithm	AES-128
IKE Hash Algorithm	SHA-1
IKE Authentication Method	RSA X.509
IPsec Encryption	AES-128
IPsec Auth	SHA-1
SA Lifetime	24 Hours

If using the DirectAccess client, it should be configured using the CPA customisation guide which is available via [CESG enquiries](#).

Both these configurations differ slightly from that of other End User Devices (which follow the PRIME and PSN interim cryptographic profiles) as they are not completely supported by Windows 7. A secondary VPN server or configuration may therefore need to be configured to run in parallel if other devices are being deployed.

8.8   AppLocker Hotfix configuration

Microsoft have released two Hotfixes which reinforce AppLocker's application whitelisting mechanism as described in [KB977542 ⬈](#) and [KB2532445 ⬈](#).

KB977542 is part of Windows 7 SP1 but requires configuration (as per this section) to enforce the AppLocker mechanism to continue to work in Safe Mode.

Settings	Value(s)
Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\Software\Microsoft\Windows\CurrentVersion\policies\system\SafeModeBlockNonAdmins	1
Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network\Appid	Service
Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network\Appid.sys	Driver
Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network\discache.sys	Driver

8.9   Protected processes

Microsoft have introduced [additional protections ⬈](#) to help mitigate [Pass-the-Hash ⬈](#) attacks in Windows 7.

This Hotfix ([KB2871997 ⬈](#)) requires configuration (as per this section) to enable the additional protections.

Settings	Value(s)
Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\LSA\RunAsPPL	1

9. Enterprise considerations

The following points are in addition to the common enterprise considerations and contain specific issues for Windows 7 deployments.

9.1 Application whitelisting

When configuring additional application whitelists for a Windows device, it is important that the following conditions are considered:

- users should not be allowed to run programs from areas where they are permitted to write files

- care should be taken to ensure that application updates do not conflict with whitelisting rules

- applications should be reviewed before being approved in the enterprise to ensure they don't undermine application whitelisting. This is especially important for scripting languages which have their own execution environment

9.2 Third party application updates

Windows Server Update Service (WSUS) can be used to deploy and update Microsoft products but cannot keep third party products up to date unless they have a package in the system management service.

9.3 Enterprise software protections

Enterprise software that handles untrusted data downloaded from the Internet through the browser needs additional protections. Application sandboxing and content rendering controls should be considered essential.

For applications such as Microsoft Office, or Adobe Acrobat, the use of their enterprise security controls should be considered. These security controls aim to help protect the end user when processing these potentially malicious files.

Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and