

## Guidance


# End User Devices Security Guidance: Windows 8.1

Updated 14 September 2015

## Contents

1. Usage scenario
2. Summary of platform security
3. How the platform can best satisfy the security recommendations
4. Network architecture
5. Deployment process
6. Provisioning steps
7. Configuration settings
8. Enterprise considerations
9. Change history

This guidance is applicable to devices running Enterprise versions of Windows 8.1, 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 8.1 Enterprise. This guidance is not applicable to Windows 8.1 RT or Windows To Go.

## 1. Usage scenario

Windows 8.1 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

## 2. 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	On supported and correctly configured hardware Windows 8.1 can support Secure boot.
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	
10. Device update policy	

### 3. How the platform can best satisfy the security recommendations

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

#### 3.1 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.

If certificates are used for user or machine credentials, it is recommended that [Windows Key Attestation](#) should also be used.

Alternatively the Windows 8.1 platform allows the use of third party VPN clients. Use a correctly configured CPA Foundation grade client.

#### 3.2 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 CESH entropy or key material is required). Deploy the BitLocker configuration settings before encryption is started.


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



“Device Encryption” introduced for Connected Standby devices in Windows 8.1 does not allow the use of a passphrase to unlock the disk and so does not support some of the mandatory requirements expected from assured disk encryption products. BitLocker or any evaluated third party product should be used instead

### **3.3 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.

### **3.4 Secure boot**

On Windows 8.1 this requirement is met on a correctly configured platform deployed on [Windows Hardware Certified](#)  hardware. 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.

### **3.5 Platform integrity and application sandboxing**


This requirement is met by the platform without additional configuration.

### **3.6 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.

A Company Store can be established to permit users access to an approved list of in-house applications. If the public Windows Store is enabled, AppLocker can be used to control which applications a user can install.

### **3.7 Malicious code detection and prevention**

Windows 8.1 includes [Windows Defender](#)  that attempts to detect malicious code for this platform. Alternatively, several third party anti-malware products are available.

Content-based attacks can be filtered by scanning capabilities in the enterprise. The Early Launch Anti-Malware (ELAM) driver, a part of Secure Boot, provides signature checking for known bad drivers on ELAM compliant systems. Note, this is only available if the platform is configured to use Secure Boot.

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

### **3.8 Security policy enforcement**

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

### **3.9 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. With Windows 8.1 connected standby devices, part of the hardware compliance mitigates DMA attacks by disallowing these interfaces.

### **3.10 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. If the Windows Store is enabled, it should be configured to automatically update Windows Store apps.

### 3.11 Event collection for enterprise analysis

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

### 3.12 Incident response

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

## 4. 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 8.1 deployments**

## 5. 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. Configure [Windows Deployment Services \(WDS\)](#) to deploy the organisations standard desktop build using a clean Windows 8.1 Enterprise image.
4. 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.


5. Deploy Group Policy settings for the organisation's chosen browser in line with the [CESG Web Browser Security Guidance](#).
6. 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.
7. 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](#) .
8. Configure user groups according to the principle of least privilege. Where available, configure these users to be in the Protected Users group and apply Restricted Admin and Authentication Policy Silos to privileged users.

## 6. 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 UEFI/BIOS to disable unused hardware interfaces, enable Secure Boot, 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.

## 7. 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 8.1 Computer Security Compliance 1.0
- MSFT Windows 8.1 User Security Compliance 1.0

Microsoft have published [Additional information](#)  discussing the changes in the baselines from Windows 8.0 to Windows 8.1.

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.

## 7.1 User configuration

Group Policy	Value(s)
User Configuration > Policies > Administrative Templates > Control Panel > Personalization > Screen saver timeout	300

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](#) .

## 7.2 Computer configuration

Group Policy	Value(s)
Computer Configuration > Policies > Administrative Templates > Control Panel > Personalization > Prevent enabling lock screen camera	Enabled
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 > Network > Network Isolation > Proxy definitions are authoritative	Enabled
Computer Configuration > Policies > Administrative Templates > Network > Network Isolation > Subnet definitions are authoritative	Enabled
Computer Configuration > Policies > Administrative Templates > System >	Enabled



Device Installation > Device Installation Restrictions > Prevent installation of devices that match these device IDs	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 > Logon > Turn off picture password sign-in	Enabled
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 > Credential User Interface > Do not display the password reveal button	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > OneDrive > Prevent the usage of OneDrive for file storage	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Portable Operating System > Windows To Go Default Startup Options	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Store > Turn off Automatic Download and Install of updates	Disabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Store > Turn off the offer to update to the latest version of Windows	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Store > Turn off the Store application	Enabled
Computer Configuration > Policies > Administrative Templates > Windows Components > Sync your settings > Do not sync	Enabled  Allow users to turn syncing on: Disabled
Computer Configuration > Policies > Administrative Templates > Windows	Enabled

Components > Tablet PC > Input Panel > Turn off password security in Input Panel	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
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Logon Option > Sign-in last interactive user automatically after a system-initiated restart	Disabled
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\LSA\RunAsPPL	1
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

## 7.3 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  
Allow Programs and Services > Service > Apply to this  
service > DHCP Client (Dhcp)  
Advanced > Profiles: Private, Public  
Allow DHCP (UDP 67/68)

General > Action: Allow the connection  
Programs and Services > Programs > This Program >  
%SystemRoot%\system32\svchost.exe  
Programs and Services > Service > Apply to this  
service > DNS Client (DNSScache)  
Advanced > Profiles: Private, Public  
Allow DNS (TCP/UDP 53)

General > Action: Allow the connection  
Programs and Services > Programs > This Program >  
%SystemRoot%\system32\svchost.exe  
Programs and Services > Service > Apply to this  
service > Network Location Awareness (NlaSvc)  
Advanced > Profiles: Private, Public  
Allow NCSI Probe (TCP 80)

General > Action: Allow the connection  
Programs and Services > Programs > This Program >  
%SystemRoot%\system32\lsass.exe  
Advanced > Profiles: Private, Public  
Allow Kerberos (TCP/UDP 88)

General > Action: Allow the connection  
Programs and Services > Programs > All Programs that  
meet the specified conditions  
Allow LDAP (TCP/UDP 389)

You may also need to add rules to allow your VPN  
client to make outbound connections when the device  
is in a public or private profile. Sample rules are  
provided with the CPA configuration guide for Direct  
Access.

---

## 7.4 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\drivers\color\ Exception: %SYSTEM32%\Spool\PRINTERS\ 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  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 > Enforcement > Script Rules	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	<p>Allow Everyone: All DLLs located in the Program Files folder</p> <p>Allow Everyone: All DLLs located in the Windows folder</p> <p>Exception: %SYSTEM32%\catroot2\*</p> <p>Exception: %SYSTEM32%\com\*</p> <p>Exception: %SYSTEM32%\com\dmpl\*</p> <p>Exception: %SYSTEM32%\FxsTmp\*</p> <p>Exception: %SYSTEM32%\powershell\*</p> <p>Exception: %SYSTEM32%\Spool\drivers\color\*</p> <p>Exception: %SYSTEM32%\Spool\PRINTERS\*</p> <p>Exception: %SYSTEM32%\Tasks\*</p> <p>Exception:</p> <p>%SYSTEM32%\Tasks\Microsoft\Windows\*</p> <p>Exception:</p> <p>%SYSTEM32%\Tasks\Microsoft\Windows\WCM\*</p> <p>Exception: %WINDIR%\debug\*</p> <p>Exception: %WINDIR%\debug\wia\*</p> <p>Exception: %WINDIR%\pchealth\*</p> <p>Exception: %WINDIR%\registration\*</p> <p>Exception: %WINDIR%\tasks\*</p> <p>Exception: %WINDIR%\temp\*</p> <p>Exception: %WINDIR%\tracing\*</p> <p>Allow Administrators: All DLLs</p>

---

Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Packaged app Rules

Configured: True Enforce Rules

---

Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > Packaged app Rules

Allow Everyone:  
windows.immersivecontrolpanel, version 6.2.0.0  
from Microsoft Corporation

Allow Everyone: winstore, version 1.0.0.0 and  
above, from Microsoft Corporation

---

## 7.5 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  
  
Configure TPM startup key and PIN:  
Allow startup key and PIN with TPM

---

## 7.6 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 > System DEP	Enabled DEP Setting: Always On

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.

## 7.7 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 profiles) as they are not completely supported by Windows 8.1. A secondary VPN server or configuration may therefore need to be configured to run in parallel if other devices are being deployed.

## 8. Enterprise considerations


The following points are in addition to the common enterprise considerations and contain specific issues for Windows 8.1 deployments.

### 8.1 Internet browser security

Modern web browsers are extremely complex software and usually have many functions beyond showing web pages. They have to process a wide variety of rich content from the Internet – some of which must be considered untrustworthy – as well as providing a trusted platform to run enterprise web apps.

It is strongly recommended that organisations read the [CESG Web Browser Security Guidance](#) to help them understand the security controls available in the most common web browsers.

### 8.2 Secure Boot

The Windows 8.1 Secure Boot process (where available on supported and correctly configured hardware) alerts a user when an attempt to subvert the security controls has taken place. It is important that users know how to [identify](#)  and respond to this alert.

### 8.3 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

## 8.4 Cloud integration


Windows 8.1 devices do not need to be associated with a Microsoft ID to operate as required within the enterprise. Users should not enable personal, non-enterprise Microsoft ID (Live ID) accounts on the device as this may allow data to leak through Microsoft cloud services backup and application storage.

However, organisations wishing to use cloud based services such as OneDrive can use the [CESG Cloud Security Guidance](#) to help them understand both the benefits and risks of using online services.

## 8.5 Windows Store applications

The configuration given above prevents users from accessing the Windows Store to install applications, but an organisation can still host its own enterprise Company Store to distribute in-house applications to their employees if required.

If the Windows Store is enabled, users should explicitly use their corporate Microsoft ID to sign into the Store app rather than associating their work device with their personal Microsoft ID. If configured as per the AppLocker configuration, AppLocker will prevent installation of apps that are not on the enterprise-configured allow list.

[Additional information](#)  on how to configure AppLocker for use with Windows Store applications is available.

## 8.6 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 enterprise system management service.

## 8.7 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.

## **9. Change history**

### **9.1 September 2015**

Firewall and AppLocker configuration has been updated fix bugs affecting some printers and the ability to auto-detect when a remote worker has their VPN active. You should apply the new configuration to existing systems if you have experienced these issues.

### **9.2 November 2014**

Some 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.

Internet Explorer configuration has been removed from this document to bring it into line with other platforms. It has been replaced by CESG's browser guidance.

## **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 organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it. This guidance is UK Crown Copyright. All Rights Reserved.

