Microsoft Windows

Common Criteria Evaluation

Microsoft Windows 10 Mobile

Microsoft Windows 10

Common Criteria Supplemental Admin Guidance

Document Information	
Version Number	1.0
Updated On	February 18, 2016

TABLE OF CONTENTS

1 Introduction

This document provides operational guidance information for a Common Criteria evaluation describing only the security functionality which the administrator should use – any security functionality not described in this document is not part of the evaluation.

1.1 Configuration

1.1.1 Evaluated Configuration

The Common Criteria evaluation includes a specific configuration of the TOE, the “evaluated configuration”. To run Windows deployments using the evaluated configuration follow the deployment steps and apply the security policies and security settings indicated below. The Security Target section 1.1 describes the Windows editions and security patches included in the evaluated configuration.

The operating system is pre-installed on the devices in the evaluated configuration. When the device is turned on for the first time the Out of Box Experience (OOBE) runs to complete the configuration.

The following security settings are applied:

- Cipher suite selection is configured according to section 5 Managing TLS
- Volume encryption is enabled according to section 7 Managing Volume Encryption
- VPN connections route all traffic through the VPN tunnel as described section 8 Managing VPN
- Passwords use a minimum of six alphanumeric characters and symbols according to sections 11.1 Strong Passwords and 11.3 Password Policy
- RSA machine certificates are configured according to section 13 Managing Certificates to use a minimum 2048 bit key length
- Session locking is enabled according to section 16 Locking a Device
- Devices are enrolled for device management according to section 17 Device Enrollment
- Enrolled policy must have the Enterprise Data Protection settings enabled

Some of the links in this document may be written for Windows versions that are earlier than Windows 10. The content in all these links apply to the Windows 10 version.

1.1.2 Mobile Device Management Solutions

Many of the configurations described in this guide for the IT Administrator role are applied to the device through a Mobile Device Management (MDM) solution. The specific steps to perform a configuration through the MDM are solution-specific and are not described in this document. Examples of possible configuration option text are provided in this document, but are not guaranteed to match any specific MDM solution. See the MDM solution documentation for detailed configuration actions.

The following link provides information about Mobile Device Management policies that MDMs may implement :

https://msdn.microsoft.com/en-us/library/windows/hardware/dn920025(v=vs.85).aspx

2 Management Functions

The following table maps management functions to roles:

	Management Function	User	Local Administrator	IT Administrator
1	Configure password policy		Windows 10	Windows 10 Windows 10 Mobile
2	Configure session locking policy		Windows 10	Windows 10 Windows 10 Mobile
3	Enable/disable the VPN protection		Windows 10	Windows 10 Windows 10 Mobile
4	Enable/disable [Wi-Fi, mobile broadband radios, Bluetooth]		Windows 10	Windows 10 Windows 10 Mobile
5	Enable/disable [camera, microphone]		Windows 10	Windows 10 Mobile Windows 10 (Camera only)
6	Specify wireless networks (SSIDs) to which the TSF may connect			Windows 10 Windows 10 Mobile
7	Configure security policy for connecting to wireless networks		Windows 10	Windows 10 Windows 10 Mobile
8	Transition to the locked state	Windows 10 Windows 10 Mobile	Windows 10	
9	TSF wipe of protected data		Windows 10	Windows 10 Windows 10 Mobile
10	Configure application installation policy		Windows 10	Windows 10 Windows 10 Mobile
11	Import keys/secrets into the secure key storage	Windows 10	Windows 10	

		Windows 10 Mobile		
12	Destroy imported keys/secrets and any other keys/secrets in the secure key storage		Windows 10	Windows 10 Windows 10 Mobile
13	Import X.509v3 certificates into the Trust Anchor Database		Windows 10	Windows 10 Windows 10 Mobile
14	Remove imported X.509v3 certificates and any other X.509v3 certificates in the Trust Anchor Database	Windows 10		Windows 10 Mobile
15	Enroll the TOE in management	Windows 10 Windows 10 Mobile		
16	Remove applications		Windows 10	Windows 10 Windows 10 Mobile
17	Update system software	Windows 10 Mobile	Windows 10	
18	Install applications		Windows 10	Windows 10 Windows 10 Mobile
19	Remove Enterprise applications		Windows 10	Windows 10 Windows 10 Mobile
20	Configure the Bluetooth trusted channel: a. disable/enable the Discoverable mode (for BR/EDR) b. change the Bluetooth device name	Windows 10 Windows 10 Mobile	Windows 10	Windows 10 Windows 10 Mobile
	d. disable/enable Advertising (for LE)			Windows 10 Windows 10 Mobile
21	Enable/disable display notification in the locked state	Windows 10 Windows 10 Mobile		
22	Enable/disable all data signaling over [**USB hardware ports**]		Windows 10	Windows 10 Windows 10 Mobile
24	Enable/disable developer modes		Windows 10	Windows 10 Windows 10 Mobile
25	Enable data-at rest protection	Windows 10 Mobile	Windows 10	
26	Enable removable media’s data at rest protection	Windows 10	Windows 10	

		Windows 10 Mobile		
28	Wipe Enterprise data	Windows 10 Windows 10 Mobile	Windows 10	
30	Configure whether to establish a trusted channel based on certificate validity	Windows 10	Windows 10	
31	Enable/disable the cellular protocols used to connect to cellular network base stations	Windows 10 Windows 10 Mobile		
33	Configure certificate used to validate digitally signed applications	Windows 10 Mobile	Windows 10	Windows 10 Windows 10 Mobile
35	Approve exceptions for destruction of keys/secrets by applications that did not import the key/secret	Windows 10 Windows 10 Mobile	Windows 10	
36	Configure the unlock banner	Windows 10 Mobile	Windows 10	
38	Retrieve TSF-software integrity verification values			Windows 10 Windows 10 Mobile
40	Enable/disable backup to remote system	Windows 10 Windows 10 Mobile	Windows 10	
44	Enable/disable location services		Windows 10	Windows 10 Windows 10 Mobile

3 Managing Wipe

This section contains the following Common Criteria SFRs:

- Extended: TSF Wipe (FCS_CKM_EXT.5)
- Specifications of Management Functions (FMT_SMF_EXT.1) : 9, 12
- Authentication Failure Handling: FIA_AFL_EXT.1.2

3.1 IT Administrator

Wipe of the TOE accomplishes removal of protected data and destruction of keys/secret. Wipe can be initiated by the MDM solution. See the MDM solution documentation for detailed configuration actions.

Windows 10 Mobile devices can be configured for wipe after exceeding a maximum number of consecutive authentication failures by the MDM administrator by using the “Number of failed logon attempts before the device is wiped” policy as described in the following TechNet topic (see “Password” heading):

- General settings for Mobile Devices in Configuration Manager: https://technet.microsoft.com/en-us/library/dn376523.aspx#BKMK_Password

The “Password” settings are enforced only if the “Require password settings on mobile devices”policy is also set.

3.2 Windows 10

3.2.1 Local Administrator Guidance

The following Windows help topic describes how to reset Windows 10 devices with removal of all user data (the “Fully clean the drive” option wipes all protected data):

How to refresh, reset, or restore your PC: http://windows.microsoft.com/en-us/windows-10/windows-10-recovery-options

4 Managing EAP-TLS

This section contains the following Common Criteria SFRs:

- Extended: Trusted Channel Communication (FTP_ITC_EXT.1)
- Extended: PAE Authentication (FIA_PAE_EXT.1)
- Extended: Trusted Channel Communication (FTP_ITC_EXT.1)
- Extended: Wireless Network Access (FTA_WSE_EXT.1)
- Specifications of Management Functions (FMT_SMF_EXT.1)

4.1 IT Administrator Guidance

An MDM system can be used to manage Wi-Fi profiles.

4.2 Windows 10

4.2.1 Local Administrator Guidance

The following topics describe how to configure EAP-TLS on Windows 10:

- Extensible Authentication Protocol (EAP) Settings for Network Access: http://technet.microsoft.com/en-us/library/hh945104.aspx[1]

The TOE comes preloaded with root certificates for various Certificate Authorities. The following TechNet topic describes how to manage trust relationships:

- Manage Trusted Root Certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx

5 Managing TLS

This section contains the following Common Criteria SFRs:

- Extended: EAP TLS Protocol (FCS_TLS_EXT.1)
- Extended: TLS Protocol (FCS_TLS_EXT.2)

The mandatory and optional cipher suites listed in the Security Target correlate with those available in the TOE as follows:

Cipher Suites (per Security Target)	**Cipher Suite Requirement**	**Available Cipher Suites in TOE[2]**
TLS_RSA_WITH_AES_128_CBC_SHA	Mandatory	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	Optional	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	Optional	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246	Optional	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256

[1] This topic also applies to Windows 10
[2] See: Cipher Suites in Schannel: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx

		and/or TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Optional	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256 and/or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384

5.1 IT Administrator Guidance

The MDM may be used to configure TLS cipher suite selection and priority.

The MDM may be used to configure the TOE to trust a Certificate Authority. The TOE comes preloaded with root certificates for various Certificate Authorities. Additional Certificate Authorities are managed on the TOE device using workplace enrollment and an MDM.Restricting Applications.

The DN in the certificate is automatically compared to the expected DN and does not require additional configuration of the expected DN for the connection.

5.2 User Guidance

Windows 10 and Windows 10 Mobile users may choose using TLS with HTTPS by using https in the URL typed into the browser.

5.3 Windows 10

5.3.1 Local Administrator Guidance

The following MSDN article describes how the administrator modifies the set of TLS cipher suites for priority and availability:

- Prioritizing Schannel Cipher Suites: http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx
- How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll: http://support.microsoft.com/kb/245030

The DN in the certificate is automatically compared to the expected DN and does not require additional configuration of the expected DN for the connection.

The TOE comes preloaded with root certificates for various Certificate Authorities. The following TechNet topic describes how to manage trust relationships:

- Manage Trusted Root Certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx

Hashes in the TLS protocol are configured in association with cipher suite selection. The administrator configures the cipher suites used on a machine by following the configuration instructions at the following link: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx

The elliptic curves supported for a particular cipher suite are part of the cipher suite configuration. For example in the table above one of the supported cipher suites is TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, note that the string used to configure this cipher suite is TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256, which is slightly different than the actual cipher suite name. The difference is the final four characters which indicate the elliptic curve that is to be used, in this case it is the curve P256 (secp256r1).

The reference identifier for TLS is the URL of the server. There is no configuration of the reference identifier.

The signature algorithm is not configurable in Windows 10 for TLS.

5.4 Windows 10 Mobile

5.4.1 User Guidance

The reference identifier for TLS is the URL of the server. There is no configuration of the reference identifier.

6 Managing Apps

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 16, 19
- Extended: Security Attribute Based Access Control (FDP_ACF_EXT.1)

6.1 IT Administrator Guidance

MDM solutions are capable of installing, removing and restricting the ability for applications to run on the TOE. See the MDM solution documentation for detailed configuration actions.

6.2 Windows 10

6.2.1 Local Administrator Guidance

The ability for users to run the Store app may be removed using a registry value on Windows 10 by performing the following steps:

1. Start the registry editor tool by executing the command regedit.exe as an administrator
2. Navigate to the registry path HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsStore. Note that the WindowsStore registry key may need to be created.

3. Create a DWORD (32 bit) registry value with the name RemoveWindowsStore under the WindowsStore registry key. Set the registry value to 1.

Local administrators can also restrict the ability of users to install applications using AppLocker on Windows 10 as described in the AppLocker Overview: https://technet.microsoft.com/en-us/library/hh831440.aspx.

The following Windows 10 help topic describes how to remove applications and any information it contained:

- Repair or remove programs: http://windows.microsoft.com/en-us/windows-10/repair-or-remove-programs#v1h=tab01

The following help topic describes the procedure to install a Windows Store app:

- Get free apps and games in Windows Store: http://windows.microsoft.com/en-us/windows-10/get-free-apps-and-games-in-windows-store

7 Managing Volume Encryption

This section contains the following Common Criteria SFRs:

- Extended: Data at Rest Protection (FDP_DAR_EXT.1)

The following TechNet topic describes the BitLocker feature, including its use to encrypt the entire operation system volume or removable volumes:

- BitLocker Overview: http://technet.microsoft.com/en-US/library/hh831713.aspx

7.1 IT Administrator Guidance

If volume encryption is enabled on the TOE, then the MDM solution can configure AES-256 encryption. See the MDM solution documentation for detailed configuration actions.

7.2 Windows 10

7.2.1 Local Administrator Guidance

The following TechNet topic describes the manage-bde command that should be executed in a command shell while running as an administrator to configure DAR protection:

- Manage-bde: http://technet.microsoft.com/en-us/library/ff829849(v=ws.10).aspx

By default AES128 encrypion is used by the manage-bde command when enabling BitLocker for Windows 10 – the AES256 algorithm should be used instead. In addition, the TPM and PIN authorization factor must be used in the evaluated configuration. The Enhanced PIN capabilities must be used in the evaluated configuration.

To enable the TPM and Enhanced PIN authorization factors execute the following command:

- `Manage-bde –on <operating system disk volume letter>: -tpmandpin -encryptionMethod aes256`

For the Surface Pro 3 and Surface 3 (LTE) a USB keyboard is necessary to enter the Enhanced PIN to unlock the drive at boot.

The following is a link to BitLocker Policy settings:

- https://technet.microsoft.com/en-us/library/jj679890.aspx

Administrators must create an Enhanced PIN value with a minimum of four and a maximum of 20 numeric characters, but can also include uppercase and lowercase English letters, symbols on an EN-US keyboard, numbers, and spaces. To enable the Enhanced PIN capabilities start the gpedit.msc MMC snap-in as an administrator and enable the following local or group policy:

- Administrative Templates\Windows Components\Bitlocker Drive Encryption\Operating System Drives\Allow enhanced PINs for startup

Other BitLocker policies that must be enabled to use the TPM and Enhanced PIN authenticator are:

- Administrative Templates\Windows Components\Bitlocker Drive Encryption\Operating System Drives\Enable use of BitLocker authentication requiring preboot keyboard input on slates
- Administrative Templates\Windows Components\Bitlocker Drive Encryption\Operating System Drives\Require additional authentication at startup

7.2.2 User Guidance

Users may use BitLocker To Go in order to encrypt removable drives. The following details how to do this:

1. Click Start, click Control Panel, click Security, and then click BitLocker Drive Encryption.

On the BitLocker Drive Encryption page, follow the instructions in the Removable data drives – BitLocker To Go section.

7.3 Windows 10 Mobile

7.3.1 User Guidance

To enable/disable Volume Encryption:

- Go to **Settings -> System -> Device Encryption**
- Tap **On/Off**

8 Managing VPN

The native Window 10 VPN client is not part of this evaluation. Windows 10 does provides support for third-party IPsec VPN clients using the Windows.Networking.Vpn classes and the networkingVpnProvider capability. The link below provides documentation for Windows.Networking.Vpn:

- https://msdn.microsoft.com/en-us/library/windows/apps/windows.networking.vpn.aspx

9 Managing Accounts

This section contains the following Common Criteria SFRs:

- Extended: Authorization Failure Handling (FIA_AFL_EXT.1)

9.1 IT Administrator Guidance

The maximum number of unsuccessful authentication attempts and associated remediation action is a Mobile Device Management (MDM) configuration policy setting that may only be managed by a Mobile Device Management system and cannot be directly configured by users on their device. If this device configuration policy setting is configured, then the remediation action wipes the device and restores factory default settings. See the MDM solution documentation for detailed configuration actions.

9.2 Windows 10

9.2.1 Local Administrator Guidance

The following TechNet topic explains the net accounts command line utility for standalone computers (followed by command line options for managing account lockout policy):

- Net Accounts: http://technet.microsoft.com/en-us/library/bb490698.aspx

In addition to the parameters given in the referenced article the following are also valid options:

/lockoutthreshold: *number* **:** Sets the number of times a bad password may be entered until the account is locked out. If set to 0 then the account is never locked out.

/lockoutwindow: *minutes* **:** Sets the number of minutes of the lockout window.

/lockoutduration: *minutes* **:** Sets the number of minutes the account will be locked out for.

Exceeding the authentication failure limit is audited by Security log Id 4740. However, this information is lost when an enrolled device exceeds the authentication failure limit configured by the IT administrator as described in section “Managing Wipe”.

10 Managing Bluetooth

This section contains the following Common Criteria SFRs:

- Extended: Bluetooth Authentication (FIA_BLT_EXT.1)
- Specifications of Management Functions (FMT_SMF_EXT.1) : 4, 20

There is no configuration that will allow Bluetooth pairing while not logged on to the TOE.

Bluetooth pairing uses a protected communication channel by default so there is no configuration necessary.

10.1 IT Administrator Guidance

The MDM solution can enable/disable Bluetooth devices on the TOE.

The MDM solution can a) disable/enable the Discoverable mode (for BR/EDR), b) change the Bluetooth device name, d) disable/enable Advertising (for LE).

10.2 Windows 10

10.2.1 Local Administrator Guidance

Bluetooth is enabled and disabled in the Settings -> Devices -> Bluetooth user interface by setting the radio button labeled Bluetooth to the On or Off state.
No configuration is necessary to ensure the Bluetooth services provided before login are limited.

10.2.2 User Guidance

Users authorize Bluetooth pairing by doing the following:

- Go to **Settings -> Devices -> Bluetooth** to open **Manage Bluetooth devices**
- Tap to select the desired Bluetooth device in the list of discovered devices indicated as **Ready to pair**
- Tap the **Pair** button to conduct the pairing operation

Users disable/enable Discoverable mode (for BR/EDR) as follows:

- Click the caret **^** icon in the taskbar, click the Bluetooth icon that is then shown in the notification area, and tap the **Open Settings** item on the context menu
- In the **Bluetooth Settings** window open the **Options** tab, check or uncheck the **Allow Bluetooth devices to find this PC** checkbox and then tap the **Apply** button

Regardless of the **Allow Bluetooth devices to find this PC** checkbox state described above, Discoverable mode is always enabled while the user is navigated to the **Settings -> Devices -> Bluetooth** settings page with the Bluetooth radio is enabled.

10.3 Windows 10 Mobile

10.3.1 User Guidance

Users authorize Bluetooth pairing by doing the following:

- Go to **Settings -> Devices -> Bluetooth** to manage the Bluetooth devices
- Tap the desired Bluetooth device in the list of discovered devices indicated as **Tap to pair** to conduct the pairing operation

Discoverable mode is always enabled while the user is navigated to the **Settings -> Devices -> Bluetooth** settings page whilewith the Bluetooth radio is enabled.

11 Managing Passwords

11.1 Strong Passwords

This section contains the following Common Criteria SFRs:

- Extended: Password Management (FIA_PMG_EXT.1)

11.1.1 IT Administrator Guidance

The composition of strong passwords and minimum password length policy settings may only be managed by a Mobile Device Management (MDM) system and cannot be directly configured by users on their device. See the MDM solution documentation for detailed configuration actions.

The following TechNet topics describe the characteristics for passwords that are available, instructions for setting the enforcement mechanism and a discussion of strong passwords and recommended minimum settings:

- Strong Password: http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx
- Password Best practices: http://technet.microsoft.com/en-us/library/cc784090(v=ws.10).aspx

11.1.2 Windows 10

11.1.2.1 Local Administrator Guidance

The following TechNet topics describe the characteristics for passwords that are available, instructions for setting the enforcement mechanism and a discussion of strong passwords and recommended minimum settings:

- Enforcing Strong Password Usage Throughout Your Organization: https://technet.microsoft.com/en-us/library/hh994562(v=ws.10).aspx
- Strong Password: http://technet.microsoft.com/en-us/library/cc756109(v=ws.10).aspx
- Password Best practices: http://technet.microsoft.com/en-us/library/cc784090(v=ws.10).aspx

11.2 Protecting Passwords

This section contains the following Common Criteria SFRs:

- Protected Authorization Feedback (FIA_UAU.7)

11.2.1 Windows 10

11.2.1.1 User Guidance

The following Windows Help topic describes how to conduct initial logon authentication for users:

- Sign in to or out of Windows: http://windows.microsoft.com/en-us/windows-8/sign-in-out-of-windows

Windows 10 do not require any configuration to ensure the password is obscured by default. The following best practices should be observed:

- As with all forms of authentication, when entering your password, avoid allowing other people to watch you as you sign in.

Keep your device in a secure location where unauthorized people do not have physical access to it. As with any password entry, be aware of line of sight and potential recording devices that intrude on your screen.

11.2.2 Windows 10 Mobile

11.2.2.1 User Guidance

Windows 10 Mobile does not require any configuration to ensure the password is obscured by default. The following best practices should be observed:

- As with all forms of authentication, when entering your password, avoid allowing other people to watch you as you sign in.
- Keep your device in a secure location where unauthorized people do not have physical access to it. As with any password entry, be aware of line of sight and potential recording devices that intrude on your screen.

11.3 Logon/Logoff Password Policy

This section contains the following Common Criteria SFRs:

- Extended: Authentication for Cryptographic Operation (FIA_UAU_EXT.1)
- Extended: Timing of Authentication (FIA_UAU_EXT.2)
- Extended: Re-Authorizing (FIA_UAU_EXT.3)
- Specifications of Management Functions (FMT_SMF_EXT.1)

11.3.1 IT Administrator Guidance

Password policies may be configured by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

11.3.2 Windows 10 Mobile

11.3.2.1 User Guidance

The following help topic describes how to configure the TSF to use (set or change) a Password Authentication Factor:

- How do I set or change a password on my phone?: http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/lock-screen-faq

Additionally, the **Require a password after** setting must be configured with the value **each time**.

11.3.3 Windows 10

11.3.3.1 Local Administrator Guidance

The out of box experience requires that when user accounts are created a password is assigned to the account.

To change an account password do either of the following:

- Tap the **Start** menu, tap the account picture, tap **Change account settings**, tap **Sign-in options**, tap **Change** under Password.
- Type the secure attention sequence: CTRL-ALT-DEL

The inactivity time period for TSF-initiated session locking is configured by the administrator via Windows security policy. The relevant security policy is “Interactive logon: Machine inactivity limit” as described in the following Technet topic in the section heading titled “New and changed functionality”:

- Security Policy Settings Overview: http://technet.microsoft.com/en-us/library/2fdcbb11-8037-45b1-9015-665393268e36

The following Technet topics include guidance for administrators to open the Local Group Policy Editor tool or the Group Policy Management Console, respectively, that are used to configure the Windows security policy:

- Local Group Policy Editor: http://technet.microsoft.com/en-us/library/dn265982.aspx

11.3.4 Windows 10 Mobile

11.3.4.1 User Guidance

Press the power button to lock the Windows 10 Mobile device.

12 Manage Lock Screen Notifications

12.1 Windows 10

12.1.1 Local Administrator Guidance

The following TechNet topics describe how to configure a message to users attempting to logon:

- Interactive logon: Message title for users attempting to log on: http://technet.microsoft.com/en-us/library/cc778393(v=ws.10).aspx
- Interactive logon: Message text for users attempting to log on: http://technet.microsoft.com/en-us/library/cc779661(v=WS.10).aspx

12.1.2 User Guidance

To manage notifications on the lock screen:

Go to Settings -> System -> Notifications & actions

12.2 Windows 10 Mobile

12.2.1 User Guidance

To enable or disable showing detailed status for applications on the lock screen:

- Go to **Settings -> Personalization**
- Tap **Lock screen**
- Then **Choose an app to show detailed status** and choose **none** from the list to receive disable receiving detailed status information, or choose an application to show its detailed status on the lock screen

To disable showing quick status for applications on the lock screen:

- Go to **Settings -> Personalization**
- Tap **Lock screen**
- Then tap each of the boxes under **Choose apps to show quick status** and then choose **none** in the **CHOOSE AN APP** screen to receive no quick status information on the lock screen, or tap a box and choose a desired application in the **CHOOSE AN APP** screen to receive quick status for that application on the lock screen

To disable receiving email, calendar or text message notifications in action center:

- Go to **Settings -> system**
- Tap N**otifications+Actions**
- Uncheck **Show notifications in action center when my phone is locked**

13 Managing Certificates

This section contains the following Common Criteria SFRs:

- Extended: Validation of Certificates (FIA_X509_EXT.1)
- Extended: Certificate Authentication (FIA_X509_EXT.2)
- Extended: Cryptographic Key Storage (FCS_STG_EXT.1)

13.1 IT Administrator Guidance

Root certificates can be added to and removed from the device using an MDM. The following link is an example of MDM documentation for certificate validation on the TOE:

- How to Deploy Certificate Profiles in Configuration Manager: https://technet.microsoft.com/en-us/library/dn270540.aspx

The TOE comes preloaded with root certificates for various Certificate Authorities. The following TechNet topic describes how to manage trust relationships:

- Manage Trusted Root Certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx

When validating a certificate with modern Windows applications the connection to a configured revocation server must be available or the validation will fail. This configuration cannot be changed.

Certificate validation for wireless network connections based on EAP-TLS is performed on the TOE using policy pushed to the device by a MDM. The following link is an example of MDM documentation for certificate validation on the TOE:

- How to Create Wi-Fi Profiles in Configuration Manager (Step 4: Configure security for the Wi-Fi profile): https://technet.microsoft.com/en-us/library/dn248970.aspx#BKMK_Step4

Certificate validation for VPN connections based on IPsec is performed on the TOE using policy pushed to the device by a MDM. The following link is an example of MDM documentation on certificate validation for VPN connections on the TOE:

- How to Create VPN Profiles in Configuration Manager (Step 4: Configure the Authentication Method for the VPN Profile): https://technet.microsoft.com/en-us/library/dn261200.aspx#BKMK_Step4

Certificate validation cannot be configured for code signing purposes.

Certificate enrollment (including certificates for client authentication) is performed on the TOE using policy pushed to the device by a MDM. The following link is an example of MDM documentation for certificate enrollment:

- Certificate Profiles in Configuration Manager: http://technet.microsoft.com/en-us/library/dn261202.aspx

Once a certificate suitable for client authentication is configured on the TOE, no additional configuration is necessary to use it.

Key lengths of keys used with certificates are configured in the certificate templates on the Certificate Authority used during enrollment and are not configured by the user or local administrator.

13.2 Developer Guidance

Application developers import and use keys and secrets with the Windows.Security.Cryptography.Certificates namespace as described by the following MSDN topic:

- Windows.Security.Cryptography.Certificates namespace: https://msdn.microsoft.com/en-us/library/windows/apps/windows.security.cryptography.certificates.aspx?f=255&MSPPError=-2147217396

Developers have a choice when enrolling for a certificate to use either CertificateEnrollmentManager base class or the derived class UserCertificateEnrollmentManager. When using UserCertificateEnrollmentManager the keys are secured by the user account credentials and user account ACLs. When using the CertificateEnrollmentManager base class the keys are only available to the application that imported or created the keys.

13.3 Shared User Keys

The following MSDN topic describes the sharedUserCertificates special capability that must be declared by Windows 10 or Windows 10 Mobile applications so that applications may share keys:

- App capability declarations: https://msdn.microsoft.com/en-us/library/windows/apps/hh464936.aspx

13.4 Windows 10

13.4.1 Local Administrator Guidance

The following TechNet topic describes managing certificates (including the “Obtain a Certificate” sub-topic):

- Manage Certificates : http://technet.microsoft.com/en-us/library/cc771377.aspx
- Certutil: http://technet.microsoft.com/library/cc732443.aspx

The operational guidance for setting up a trusted channel to communicate with a CA is described in the operational guidance for FTP_ITC.1 (OS)).

The TOE comes preloaded with root certificates for various Certificate Authorities. The following TechNet topic describes how to manage trust relationships:

- Manage Trusted Root Certificates: http://technet.microsoft.com/en-us/library/cc754841.aspx

The following TechNet topic describes how to delete a certificate:

- Delete a Certificate: http://technet.microsoft.com/en-us/library/cc772354.aspx

Root certificates can be added to and removed from devices using an MDM for enrolled devices.

When validating a certificate with modern Windows applications the connection to a configured revocation server must be available or the validation will fail. This configuration cannot be changed.

The administrator configures certificate validation using the Set-NetFirewallSetting PowerShell cmdlet as described in the following TechNet topic:

- Set-NetFirewallSetting: http://technet.microsoft.com/en-us/library/jj554878.aspx

The administrator configures certificate validation for network connections based on EAP-TLS using the “Set Up a Connection or Network” wizard in the “Smart Card or Other Certificate Properties” and “Configure Certificate Selection” screens as described in the following TechNet topic:

- Extensible Authentication Protocol (EAP) Settings for Network Access (Smart Card or other Certificate Properties configuration items): https://technet.microsoft.com/en-us/library/hh945104.aspx#BKMK_LAN_SmartCard

The administrator configures certificate validation for HTTPS using the Security options checkboxes in the Advanced tab on the Internet Properties dialog for Control Panel. The “Warn about certificate address mismatch” setting configures whether the Web address must match the certificate subject field and warns the user of a mismatch. The following MSDN Blog describes the “Check for server certificate revocation” setting:

- Understanding Certificate Revocation Checks: http://blogs.msdn.com/b/ieinternals/archive/2011/04/07/enabling-certificate-revocation-check-failure-warnings-in-internet-explorer.aspx

The administrator cannot configure certificate validation for code signing purposes.

Key lengths of keys used with certificates are configured in the certificate templates on the Certificate Authority used during enrollment and are not configured by the user or local administrator.

13.4.2 User Guidance

The following TechNet topic describes how to manually import a certificate:

- Import a Certificate: http://technet.microsoft.com/en-us/library/cc754489.aspx

Keys are deleted using device wipe as described in section Managing Wipe.

When using HTTPS in a browsing scenario the user may choose to ignore a failed certificate validation and continue the connection.

13.4.3 Custom Certificate Requests

Certificate requests with specific fields such as "Common Name", "Organization", "Organizational Unit", and/or "Country" can be generated by apps using the Certificates.CertificateEnrollmentManager.CreateRequestAsync API. The following link provides the documentation for the API:

- https://msdn.microsoft.com/en-us/library/windows/apps/windows.security.cryptography.certificates.certificateenrollmentmanager.createrequestasync.aspx

13.5 Windows 10 Mobile

13.5.1 User Guidance

Keys are deleted using device wipe as described in section Managing Wipe.

14 Managing Time

This section contains the following Common Criteria SFRs:

- Reliable Time Stamps (FPT_STM.1)

14.1 Windows 10

14.1.1 Local Administrator Guidance

The administrator sets the time using the Set-Date PowerShell cmdlet that is documented here:

- http://technet.microsoft.com/en-us/library/7f44d9e2-6956-4e55-baeb-df7a649fdca1

The administrator configures the time service to synchronize time from a time server using the W32tm command that is documented here:

- http://technet.microsoft.com/en-us/library/cc773263(v=WS.10).aspx#w2k3tr_times_tools_dyax

The administrator ensures the communication path between the TOE client and the time service provider is protected from attacks that could compromise the integrity of the time by establishing an IPsec policy using the “Microsoft Windows 8 Microsoft Windows Server 2012 --- Supplemental Admin Guidance for IPsec VPN Clients (January 23 2014)”, where section 3 provides detailed instructions that can be used to configure the TOE client and the time service provider.

The administrator ensures the NTP server is authenticated by verifying the IP address provided by the IT administrator for the NTP Server in the main mode and quick mode security associations according to the audit trail for the FTP_ITC.1 requirement outlined in section "4.1 Audit Policy for IPsec Operations" of the IPsec VPN Client guidance. In particular, audits are provided when a trusted channel is established that includes the IP address of the channel's local and remote endpoints. If the integrity of the trusted channel is compromised, then this is indicated by the audit Id 4960 that is also discussed in section 4.1.

14.2 Windows 10 Mobile

14.2.1 User Guidance

To set the time on Windows 10 Mobile :

- Go to **Settings -> Time & Language -> Date & Time**
- Then enable **Set date and time automatically** or set the time manually.

Windows 10 Mobile also supports automatically setting the date and time by the mobile operator via Network Identity and Time Zone (NITZ). Otherwise if the mobile operator does not support NITZ, then the user can only configure the date and time manually.

Windows 10 Mobile devices do not support NTP.

15 Getting Version Information

This section contains the following Common Criteria SFRs:

- Extended: Trusted Update: TSF Version Query (FPT_TUD_EXT.1)

15.1 Windows 10

15.1.1 User Guidance

To determine the hardware model and operating system version:

- Go to Settings -> System -> About

The following are instructions for getting the version of an app on Windows 10:

1. Start the app you wish to get the version of.

2. Once the app is opened, move your mouse cursor to the upper-right or lower-right corner of the screen to see the Charms bar. Touch screen users need to swipe-in from the right-edge of the screen to bring up the Charms bar.
3. Click or tap Settings charm on the Charms bar to open Settings for the app.

Click or tap **Permissions** to see the developer's name and also current version of the app.

15.2 Windows 10 Mobile

15.2.1 User Guidance

To determine the hardware model and operating system version :

- Go to **Settings -> System -> About**
- The hardware model and operating system version will be displayed on this page.

The following steps describe how to determine the version of apps on the device:

1. Open the app
2. Tap More… , then tap Settings.
3. The version of the app will be displayed on this page.

16 Locking a Device

This section contains the following Common Criteria SFRs:

- Extended: TSF and User initiated Locked State (FTA_SSL_EXT.1)
- Specifications of Management Functions (FMT_SMF_EXT.1) : 2, 3, 8

16.1 IT Administrator Guidance

Session locking policies may be configured by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

16.2 Windows 10

16.2.1 User Guidance

To initiate a session lock:

- Tap the **Start** menu, tap the account picture, click **Lock**.

16.3 Windows 10 Mobile

16.3.1 User Guidance

The device may be commanded to transition to the locked state by configuring the inactivity interval as above and then pressing the button to power off the device such that the lock screen will be presented and the password will be required when the button is pressed to turn the device back on.

The following TechNet topic describes the configuration of notifications in the locked state:

- Locked phone: things it can still do: http://www.windowsphone.com/en-us/how-to/wp8/settings-and-personalization/locked-phone-things-it-can-still-do

17 Managing Device Enrollment

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 19
- Extended: Specification of Remediation Actions (FMT_SMF_EXT.2)

Unenrollment from the MDM solution performs the remediation actions of:

- alert the administrator
- remove Enterprise applications

17.1 Windows 10

17.1.1 Local Administrator Guidance

To enroll for management do the following

- Go to Settings -> Accounts -> Work access
- Tap the Connect button
- Fill in the user account credentials provided by your IT administrator

To unenroll from device management do the following:

- Go to Settings > Account -> Work access
- Tap the Remove button that is displayed when the enrollment setting is selected, and then confirm the Remove operation

The local administrator determines if the device is enrolled or not enrolled by looking at the Work access page of the Accounts settings. On the Work access page of the Accounts settings if the device device is enrolled then the enrollment setting is indicated by the Work access name as established by your IT administrator and your account name provided by your IT administrator that was used to enroll the device – tapping the enrollment setting reveals the Sync, Info and Remove buttons that may be used to synchronize device management settings, inspect Work access enrollment settings or remove the device from enrollment.

17.1.2 User Guidance

Users manage device enrollment like local administrators as described above.

17.2 Windows 10 Mobile

17.2.1 User Guidance

The following describes how to enroll and unenroll with an MDM. A MDM can wipe a device during unenroll.

To add a workplace account

- Go to **Settings -> Accounts.**
- Tap **Work access.**
- Tap **Connect.**
- Enter your work email address, and then tap **Connect.**
- Enter your password, if prompted. Otherwise follow the instructions on the screen.

Note

The process for adding a workplace account to your device might be different where you work. For example, you might be taken to an employer website to finish setting up your account.

- If your employer offers a company app or hub, you'll see an option to add it once your account is set up. New apps appear in your App list.

Notes

You can only add one workplace account at a time on your device.

To delete a workplace account

- Go to **Settings -> Accounts.**
- Tap and hold the account you want to remove.
- Tap the Delete Settings icon, and then tap the **Remove** button.

To sync a workplace account

- Go to **Settings -> Accounts.**
- Tap and hold the account you want to sync.
- Tap the Sync button.

18 Managing Updates

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 17
- Operational User Guidance (AGD_OPE)

Windows applications include metadata that is installed with the application by the Windows Installer and the Store App installer. The application metadata includes version information that prevents the Windows Installer and the Store App installer from updating an installed application with an older version.

Update packages downloaded by the TOE are signed with the Microsoft Root Certificate Authority to prove their authenticity and integrity. This signature is checked on the mobile device before installing any of the product updates contained in a given package in order to verify the updates have not been altered since they where digitally signed. If the signature is incorrect, then the update operation will fail. Otherwise, if the signature is correct then the update operation will proceed. The user guidance indicated in the links below tell how to determine if an update operation was successful or unsuccessful.

18.1 Windows 10

18.1.1 Local Administrator

To configure System Updates:

- Go to Settings -> Update & security -> Windows Update

18.2 Windows 10 Mobile

18.2.1 User Guidance

The following link describes how to get updates on Windows 10 Mobile:

http://www.windowsphone.com/en-us/how-to/wp8/update-central

19 Managing Collection Devices

19.1 IT Administrator

The camera may be enabled/disabled on the TOE by using a Mobile Device Management (MDM) solution. The microphone may be enabled/disabled on Windows 10 Mobile by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

19.2 Windows 10

19.2.1 Local Aministrator Guidance

The local administrator disables/enables the camera for all users by disabling all subnodes under the “Imaging devices” node in the Device Manager.

To start the Device Manager, type “Device Manager” in the taskbar searchbox and click on the **Device Manager** icon.

The local administrator disables/enables the microphone for all users by the following procedure:s

1. On the desktop right click on the Start button and click the Control Panel menu item.
2. Type “Sound” and choose “Manage audio devices” from the list to open the Sound window
3. In the Sound window click the “Recording” tab

4. On the Recording tab right the Microphone item(s) and select the “Disable” menu item
   Note: to reverse this step the “Show Disabled Devices” menu item should be selected.

20 Managing Backup

20.1 Windows 10

20.1.1 User Guidance

The following Windows 10 topic describes how to configure Backup and Restore: http://windows.microsoft.com/en-us/windows-10/getstarted-back-up-your-files

The following Windows 10 topic describes how to configure OneDrive to sync files and folders: http://windows.microsoft.com/en-us/windows-10/getstarted-onedrive

To configure OneDrive to sync settings: Settings -> Accounts -> Sync your settings.

20.2 Windows 10 Mobile

20.2.1 User Guidance

The following help topic describes how to disable the “Sync my settings” feature:

- Sync my Windows Phone settings: http://www.windowsphone.com/en-US/how-to/wp8/settings-and-personalization/sync-my-windows-phone-settings

21 Managing Cryptographic Algorithms

21.1 User Guidance

This guidance applies to both Windows 10 and Windows 10 Mobile.

There is no global configuration for hashing algorithms. The use of required hash sizes is supported and global configuration is not needed.

There is no global configuration for key generation schemes. The use of required key generation schemes is supported and global configuration is not needed.

There is no global configuration for key establishment schemes. The use of required key establishment schemes is supported and global configuration is not needed.

Keys may be imported by apps using the Certificates.CertificateEnrollmentManager.ImportPfxDataAsync API. The following link provides the documentation for the API:

- https://msdn.microsoft.com/en-us/library/windows/apps/windows.security.cryptography.certificates.certificateenrollmentmanager.importpfxdataasync.aspx

Keys are destroyed by wiping the device, see the Managing Wipe section of this document.

The Windows 10 system cryptographic engine was tested during the FIPS evaluation of the operating system. Other cryptographic engines may have been separately evaluated but were not part of this CC evaluation.

22 Managing Location Services (GPS)

22.1 IT Administrator

GPS may be enabled/disabled on the TOE by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

22.2 Windows 10

22.2.1 Local Administrator Guidance

Configure Location Services: http://windows.microsoft.com/en-us/windows-10/location-service-privacy

Click **Change**.

23 Managing Wi-Fi

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 6
- Specifications of Management Functions (FMT_SMF_EXT.1) : 4

23.1 IT Administrator

Wi-Fi may be enabled/disabled on TOE by using a Mobile Device Management (MDM) solution. Wi-Fi SSIDs may be configured on the TOE by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

23.2 Windows 10

23.2.1 Local Administrator Guidance

Enable/disable the wireless network adapter: http://windows.microsoft.com/en-us/windows/enable-disable-network-adapter#1TC=windows-7

23.3 Windows 10 Mobile

23.3.1 User Guidance

To enable Wi-Fi:

- Go to **Settings -> Network & Wireless**
- Tap **Wi-Fi**
- Then turn it on

24 Managing Developer Mode

24.1 IT Administrator

Consult MDM documentation for enabling/disabling Developer mode with an MDM.

24.2 Windows 10

24.2.1 Local Administrator Guidance

Developer Mode allows installation of test-signed applications. The local administrator or user configures Developer Mode in Settings -> Updates & security -> For developers by selecting the Developer Mode radio button.

25 Managing Health Attestation

The contents of the Health Attestation logs may be viewed on or off the TOE using the “TPM Platform Crypto-Provider Toolkit” that can be downloaded from the following link:

TPM Platform Crypto-Provider Toolkit : http://research.microsoft.com/en-us/downloads/74c45746-24ad-4cb7-ba4b-0c6df2f92d5d/

25.1 IT Administrator Guidance

MDM solutions are capable of managing Health Attestation on the TOE including the Health Attestation log. See the MDM solution documentation for detailed configuration actions.

25.2 Windows 10

25.2.1 Local Administrator Guidance

The device will create a Helath Attestation log every time the system boots. The Health Attestation logs are found in the following directory:

%windir%\Logs\MeasuredBoot

26 Managing USB

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 22

26.1 IT Administrator Guidance

MDM solutions are capable of managing USB connectivity on devices. See the MDM solution documentation for detailed configuration actions.

26.2 Windows 10

26.2.1 Local Administrator

The following link describes how to enable/disable installation restrictions of USB removable devices for Windows 10:

- Managing Hardware Restrictions via Group Policy: https://technet.microsoft.com/en-us/magazine/2007.06.grouppolicy.aspx

The local administrator may also disable the USB in the Device Manager application by right-clicking the USB Root Hub child node in the Universal Serial Bus controllers node and selecting the Properties menu item to open the USB Root Hub Properties window. the local administrator then clicks the Driver tab In the USB Root Hub Properties window and clicks he Disable button.

27 Managing Notifications Prior to Unlocking a Device

This section contains the following Common Criteria SFRs:

- Default TOE Access Banners (FTA_TAB.1)
- Specifications of Management Functions (FMT_SMF_EXT.1) : 36

27.1 Windows 10

27.1.1 Local Administrator Guidance

The following TechNet topics describe how to configure a message to users attempting to logon:

- Interactive logon: Message title for users attempting to log on: http://technet.microsoft.com/en-us/library/cc778393(v=ws.10).aspx
- Interactive logon: Message text for users attempting to log on: http://technet.microsoft.com/en-us/library/cc779661(v=WS.10).aspx

27.2 Windows 10 Mobile

27.2.1 User Guidance

- Distribute a photo to all users that has a picture with the notice and consent warning message.
- Each user then does the following on the device:

1. In the App list, tap **Settings**.
2. In the Settings list tap **lock screen**.
3. Under **Background** tap **choose background**.
4. Tap **photo**.
5. Tap **change photo**.
6. Select and tap the photo distributed by the administrator and tap the check mark at the bottom of the photo.

The device with the notice and consent warning is now displayed before unlocking the device.

28 Managing Mobile Broadband

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 31

28.1 User Guidance

Settings for enabling/troubleshooting Mobile Broadband: http://windows.microsoft.com/en-us/windows-10/cellular-settings

29 Manage Session Locking Policy

This section contains the following Common Criteria SFRs:

- Specifications of Management Functions (FMT_SMF_EXT.1) : 2

29.1 IT Administrator Guidance

Screen lock timeout configuration may be configured on the TOE by using a Mobile Device Management (MDM) solution. See the MDM solution documentation for detailed configuration actions.

As an example, the following TechNet topic describes the “Idle time before mobile device is locked (minutes)” MDM configuration policy setting that may be used to configure the “MaxInactivityTimeDeviceLock” MDM configuration policy settings for enrolled devices:

- Compliance Settings for System Center 2012 R2 Configuration Manager: http://technet.microsoft.com/en-us/library/dn376523.aspx#bkmk_comps

29.2 Windows 10

29.2.1 Local Administrator Guidance

The following Technet topics include guidance for administrators to open the Local Group Policy Editor tool or the Group Policy Management Console, respectively, that are used to configure the Windows security policy for standalone or domain-joined machines:

- Local Group Policy Editor: http://technet.microsoft.com/en-us/library/dn265982.aspx
- Group Policy Management Console: http://technet.microsoft.com/en-us/library/dn265969.aspx

The inactivity time period for TSF-initiated session locking is configured by the administrator via Windows security policy. The relevant security policy is “Interactive logon: Machine inactivity limit” as described in the following Technet topic in the section heading titled “New and changed functionality”:

- Security Policy Settings Overview: http://technet.microsoft.com/en-us/library/2fdcbb11-8037-45b1-9015-665393268e36