Microsoft Windows

Common Criteria Evaluation

Microsoft Windows 10

Microsoft Windows Server 2012 R2

Common Criteria Supplemental Admin Guidance

Document Information	
Version Number	0.09
Updated On	January 13, 2016

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Serverare either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

1 Introduction

This document provides operational guidance information for a Common Criteria evaluation.

This document provides many links to TechNet and other Microsoft resources which often include an “Applies to:” list of operating system versions. For each such link in this document it has been verified that the link applies to the Windows Operating System (OS) versions listed in the following section.

1.1 Evaluated Windows Editions and Hardware Platforms

This operational guide applys to the following Windows Operating Systems (OS) editions that were tested as part of the evaluated configuration:

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 R2 Standard Edition
- Microsoft Windows Server 2012 R2 Datacenter Edition

As part of the Common Criteria evaluation, the following real and virtualized hardware platforms test as part of the evaluated configuration:

- Microsoft Surface Book
- Microsoft Surface Pro 3
- Microsoft Surface 3
- Windows Server 2012 R2 Hyper-V
- HP Pro x612 Notebook PC
- Dell OptiPlex 755

1.2 Configuration

1.2.1 Evaluated Configuration

The Common Criteria evaluation includes a specific configuration of Windows, 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 security patches that must be included in the evaluated configuration.

The operating system may be 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 initial configuration.

The operating system may also be installed from installation media as described below.

The following Windows help topic has procedures to download Windows 10 installation media as an ISO file for installation and to install the operating system:

- Get Windows 10: https://www.microsoft.com/en-us/software-download/windows10

The following MSDN topic has procedures to download Windows Server 2012 R2 installation media as an ISO file that may be used for either the DataCenter or Standard editions, depending upon the licensing information that is provided during installation:

- Download Windows Server 2012 R2: https://msdn.microsoft.com/en-us/windowsserver2012r2.aspx

Bootable media may be created for both Windows 10 and Windows Server 2012 R2 using the instructions at the following link (see the “I’ve downloaded an ISO, now what?” topic):

- Software Download : https://www.microsoft.com/en-us/software-download/faq

Windows 10 and Windows Server 2012 R2 may be installed using the instructions at the following link (see the “I’ve created media using the media creation tool, now what do I do?” topic):

- Software Download : https://www.microsoft.com/en-us/software-download/faq

1.2.1.1 Managing User Roles

The evaluated configuration includes two user roles:

- Local Administrator – A user account that is a member of the local Administrators group
- User – A standard user account that is not a member of the local Administrators group

Access to user-accessible functions is controlled by the rights and privileges assigned to these two user roles. No additional measures are needed to control access to the user-accessible functions in a secure processing environment. Attempts to access user-accessible functions that requirelocal administrator rights or privileges are denied for the user role.

The following Technet topic describes how to make a standard user account a member of the local Administrators group:

- Add a member to a local group: https://technet.microsoft.com/en-us/library/cc772524.aspx

The operational guidance includes sections for “Local Administrator Guidance” and “User Guidance” that correspond to the two user roles. In these sections the available security functionality and interfaces, including all security parameters, are indicated as appropriate for each role.

1.2.1.2 Setup Requirements

The following security policies must beapplied by an administrator after completing the OOBEin order to fulfil the security objectives for the evaluated configuration:

Security Policy	Policy Setting
Local Policies\Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm	Enabled
Administrative Template\Windows Components\Credentials User Interface\Do not display the password reveal button	Enabled

The following security settings must also beappliedin order to fulfil the security objectives for the evaluated configuration:

- Cipher suite selection must be configured according to Section 4 Managing TLS
- Complex passwords must be configured as described inSection 6Managing Passwords
- RSA machine certificates must beconfigured according to Section 7 Managing Certificates to use a minimum 2048 bit key length
- Session locking must be enabled according to section 8 Locking a Device
- Hibernation must be disabled according to section 20 Managing Hibernation

To install and maintain the operating system in a secure state the following guidance must be observed:

- Windows 10 and Windows Server 2012 R2 must be installed on trusted hardware platforms
- Users must use a separate account that is a member of the local Administrators group to perform the procedures in sections of this documentlabeled as “Local Administrator Guidance”
- Administators must utilize the guidance included in this document to administer the TOE

1.2.1.3 Modes of Operation

There are four modes of operation:

- Operational Mode – The normal mode of operation when the system has booted.
- Non-Operational Mode – The mode where the system has not booted normally. In this mode the system is not operational and must be reinstalled.
- Debug Mode – The mode where the Windows boot optionsare configured to enablekernel debugging of the operating system
- Safe Mode – The mode where Windows boot options are configured to to start the operating system in a limited state where only essential programs are loaded

Only the operational mode, the normal mode of operation first noted above, is the evaluated mode.

2 Management Functions

The following table maps management functions to sections in this document.As indicated by the “Local Administrator” and “User” columns, some management functions have activities that may only be performed by a local administrator while others also have activities that may be performed by a standard user. Rows indicated with ~~strikethrough~~ text indicate Common Criteria requirements that were not included in the evaluated configuration.

#	Activity	Section	Local Administrator	User
1	configure minimum password length	6	√	
2	~~configure minimum number of special characters in password~~	-		
3	~~configure minimum number of numeric characters in password~~	-		
4	~~configure minimum number of uppercase characters in password~~	-		
5	~~configure minimum number of lowercase characters in password~~	-		
6	enable/disable screen lock	8	√	√
7	configure screen lock inactivity timeout	8	√	√
8	configure remote connection inactivitytimeout	8	√	
9	~~enable/disable unauthenticated logon~~	-		
10	configure lockout policy for unsuccessful authentication attempts through [**selection**:*timeouts between attempts, limiting number of attempts during a time period*]	5	√	
11	configure host-based firewall	13	√	
12	configure name/address of directory serverto bind with	14	√	
13	configure name/address of remotemanagement server from which to receivemanagement settings	14	√	
14	~~configure name/address of audit/logging server to which to send audit/logging records~~	-		
15	configure local audit storage capacity	3	√	
16	configure audit rules	3	√	
17	configure name/address of network timeserver	15	√	
18	enable/disable automatic software update	12	√	

19	configure WiFi interface	16	√	
20	enable/disable Bluetooth interface	10	√	
21	configure USB interfaces	11	√	
22	enable/disable [**local area network interface**]	9	√	

3 Managing Audits

3.1 Audit Events

This table lists the set of audits that were tested in the evaluated configuration.

Description	**Id**
Authentication events (Success/Failure)	Windows Logs/Security: Success: 4624 Failure: 4625
Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)	Windows Logs/Security: WRITE_DAC : 4670 All other object access writes : 4656
Privilege or role escalation events (Success/Failure)	Windows Logs/Security: 4673, 4674
File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)	Windows Logs/Security: 4656
User and Group management events (Successful and unsuccessful add, delete, modify, suspend, lock)	Windows Logs/Security: add user: 4720 add user to group: 4732 delete user: 4726 delete user from group: 4733 add group: 4731 delete group: 4734 modify group: 4735 modify user account: 4738 disable user: 4725
Lock and unlock a user account	Lock: 4740

	Unlock: 4767
Audit and log data access events (Success/Failure)	Windows Logs/Security: 4674
Cryptographic verification of software (Success/Failure)	Windows Logs/Setup: Failure: 3 Success: 2
Program initiations (Success/Failure e.g. due to software restriction policy)	Device Guard Microsoft-Windows-CodeIntegrity/Verbose Success: 3038 Microsoft-Windows-CodeIntegrity/Operational Failure: 3077 AppLocker Microsoft-Windows-AppLocker/Packaged app-Execution Success: 8020 Failure: 8022
System reboot, restart, and shutdown events (Success/Failure),	Windows Logs/Security: 4608, 1100
Kernel module loading and unloading events (Success/Failure),	Boot kernel module loading success: Windows Boot Configuration Log Other kernel module loading success: Microsoft-Windows-CodeIntegrity/Verbose: 3038 Boot kernel module loading failure: Recovery Screen Other kernel module loading failure: Microsoft-Windows-CodeIntegrity/Operational: 3004
Administrator or root-level access events (Success/Failure),	Success: Windows Logs/Security: 4624 Failure: Windows Logs/Security: 4625

The table below lists the details of each event listed in the table above.

Id	Log location	Message	Fields
2	Windows Logs ->Setup	Package was successfully changed to the Installed state	Logged: <Date and time of event> PackageIdentifier: <KB package Id> IntendedPackageState: Installed ErrorCode: <success outcome indicated by 0x0>

3	Windows Logs ->Setup	Windows update could not be installed because … “The data is invalid”	Logged: <Date and time of event> Commandline: <KB package Id> ErrorCode: <install failure indicated by 0x800700D (2147942413)>
1100	Windows Logs -> Security Subcategory: Security State Change	The event logging service has shut down	Logged: <Date and time of event> Keywords: <Outcome as Success>
3004	Microsoft-Windows-CodeIntegrity/Operational	Windows is unable to verify the image integrity of the file <pathname> because the file hash could not be found on the system.	Logged: <Date and time of event> Keywords: <Outcome as Failure> FileNameBuffer: <pathname>
3038	Microsoft-Windows-CodeIntegrity/Verbose	Code Integrity started validaging image header of <kernel module pathname> file	Logged: <Date and time of event> Keywords: <Outcome as Success> FilenameBuffer: <kernel module pathname>
3077	Microsoft-Windows-CodeIntegrity/Operational	Code Integrity determined that a process <process name> attempted to load <target process name> that did not meet the Enterprise signing level requirements or violated code integrity policy.	Logged: <Date and time of event> Keywords: <Outcome as Failure> Filename: <target process filename> Process name: <target process name>
4608	Windows Logs -> Security Subcategory: Security State Change	Startup of audit functions	Logged: <Date and time of event> Task category: <type of event> Keywords: <Outcome as Success or Failure>
4624	Windows Logs/Security Subcategory: Logon	An account was successfully logged on.	Logged: <Date and time of event> Security ID: <SID of enabled user account> Account Name: <name of enabled account> Account Domain: <domain of enabled account if applicable, otherwise computer> Workstation Name: <name of computer user logged on> Logon Type: <type of logon (e.g. interactive)> LogonID: <unique logon identification> Source Network Address: <IP address of computer logged on>
4625	Windows Logs/Security Subcategory: Logon	An account failed to log on.	Logged: <Date and time of event> Security ID: <SID of user account that failed to logon> Account Name: <name of account that failed to logon> Account Domain: <account domain that failed to logon if applicable, otherwise computer> Logon Type: <type of logon (e.g. interactive)>

4656	Windows Logs/Security Subcategory: Handle Manipulation	A handle to an object was requested.	Logged: <Date and time of event> Security ID: <SID of locked account> Object Name: <Pathname of the object changed> Accesses: <Access granted (for success event) or denied (for failure event)> Access Mask: <Access requested> Keywords: <Outcome as Success or Failure>
4670	Windows Logs -> Security Subcategory: Policy Change	Permissions on an object were changed.	Logged: <Date and time of event> Security ID: <SID of user account that viewed the log> Account Name: <user account name that viewed the log> Account Domain: <domain of user accout that viewed the log> Object Name: <Pathname of the object changed> Original security descriptor: <security descriptor> New security descriptor: <security descriptor> Keywords: < Outcome as Success or Failure>
4673	Windows Logs -> Security Subcategory: Sensitive Privilege Use / Non Sensitive Privilege Use	A privileged service was called.	Logged: <Date and time of event> Security ID: <SID of user account that viewed the log> Account Name: <user account name that viewed the log> Account Domain: <domain of user accout that viewed the log> Keywords: < Outcome as Success or Failure>
4674	Windows Logs/Security Subcategory: Sensitive Privilege Use / Non Sensitive Privilege Use	An operation was attempted on a privileged object.	Logged: <Date and time of event> Security ID: <SID of user account that attempted the operation> Account Name: <user account name that attempted the operation> Account Domain: <domain of user accout that viewed the log, if applicable, otherwise computer name> Keywords: <Outcome as Success or Failure>
4720	Windows Logs/Security Subcategory: User Account Management	A user account was created.	Logged: <Date and time of event> Security ID: <SID of new account> Account Name: <name of new account> Keywords: <Outcome as Success or Failure>

4725	Windows Logs/Security Subcategory: User Account Management	A user account was disabled.	Logged: <Date and time of event> Security ID: <SID of account> Account Name: <name of account> Keywords: <Outcome as Success or Failure>
4726	Windows Logs/Security Subcategory: User Account Management	A user account was deleted.	Logged: <Date and time of event> Security ID: <SID of deleted account> Account Name: <name of deleted account> Keywords: <Outcome as Success or Failure>
4731	Windows Logs/Security Subcategory: User Account Management	A security-enabled local group was created.	Logged: <Date and time of event> Group SID: <SID of group> Group Name: <Name of group> Keywords: <Outcome as Success or Failure>
4732	Windows Logs/Security Subcategory: User Account Management	A member was added to a security-enabled group.	Logged: <Date and time of event> Member SID: <SID of user account> Group SID: <SID of group> Account Name: <name of user account> Group Name: <Name of group> Group SID Keywords: <Outcome as Success or Failure>
4733	Windows Logs/Security Subcategory: User Account Management	A member was removed from a security-enabled group.	Logged: <Date and time of event> Member SID: <SID of user account> Group SID: <SID of group> Account Name: <name of user account> Group Name: <Name of group> Group SID Keywords: <Outcome as Success or Failure>

4734	Windows Logs/Security Subcategory: User Account Management	A security-enabled local group was deleted.	Logged: <Date and time of event> Group SID: <SID of group> Group Name: <Name of group> Keywords: <Outcome as Success or Failure>
4735	Windows Logs/Security Subcategory: User Account Management	A security-enabled local group was changed.	Logged: <Date and time of event> Group SID: <SID of group> Group Name: <Name of group> Keywords: <Outcome as Success or Failure>
4738	Windows Logs/Security Subcategory: User Account Management	A user account was changed	Logged: <Date and time of event> Security ID: <user identity>
4740	Windows Logs/Security Subcategory: Account Lockout	A user account was locked out.	Logged: <Date and time of event> Security ID: <SID of user account> Account Name: <name of user account> Account Domain: <domain of locked user account if applicable, otherwise computer>
4767	Windows Logs/Security Subcategory: Account Lockout	A user account was unlocked.	Logged: <Date and time of event> Security ID: <SID of user account> Account Name: <name of unlocked account> Account Domain: <domain of unlocked account>
8020	Microsoft-Windows-AppLocker/Packaged app-Execution	<Packaged app name> was allowed to run.	Logged: <Date and time of event> RuleAndFileData: <Packaged app name, rule Id, etc.>
8022	Microsoft-Windows-AppLocker/Packaged app-Execution	<Packaged app name> was prevented from running.	Logged: <Date and time of event> RuleAndFileData: <Packaged app name, rule Id, etc.>

3.2 Managing Audit Policy

3.2.1 Local Administrator Guidance

The following log locations are always enabled:

- Windows Logs -> System
- Windows Logs -> Setup
- Windows Logs -> Security (for startup and shutdown of the audit functions and of the OS and kernel, and clearing the audit log)

The following TechNet topic describes the categories of audits in the Windows Logs -> Security log:

- Advanced Audit Policy Configuration: http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx

The following TechNet topic describes how to select audit policies by category, user and audit success or failurein the Windows Logs -> Security log:

- Auditpol set: https://technet.microsoft.com/en-us/library/cc755264.aspx

For example, to enable all audits in the given subcategoriesof the Windows Logs -> Security log run the following commands at an elevated command prompt:

- Logon operations:
  auditpol /set /subcategory:”Logon” /success:enable /failure:enable

- audit policy changes:
  auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable

- Configuring IKEv1 and IKEv2 connection properties:
  auditpol /set /subcategory:"Filtering Platform Policy Change" /success:enable /failure:enable
  auditpol /set /subcategory:"Other Policy Change Events" /success:enable /failure:enable

- registry changes (modifying TLS Cipher Suite priority):
  auditpol /set /subcategory:"Registry" /success:enable /failure:enable

In addition to enabling audit policy as noted above, each registry key or other system object to be audited must also have its auditing permissions set by changing the System Access Control List (SACL) for that object. The process is slightly different for each object type to be audited. For example, to set the SACL for a registry object:

1. Start the registry editor tool by executing the command regedit.exe as an administrator
2. Navigate to the registry path for the key that should be audited, right-click the key's node and select **Permissions…** on the key's context menu to open the **Permissions** dialog
3. Click the **Advanced** button to open the **Advanced Security Settings** dialog, click on the **Auditing** tab and click the **Add** button to open the **Auditing Entry** dialog
4. Click the **Select a principal** to open the **Select User or Group** dialog to select a user (e.g. Administrator) and click the OK button.
5. Choose the desired audits using the **Type**, **Applies to** and **Basic Permissions** attributes and click **OK**
6. Click **OK** on the **Advanced Security Settings** dialog
7. Click OK on the **Permissions** dialog

For a file object, open the properties dialog for a file object, click **Security**, click **Advanced**, and click **Auditing**.

For more information, the following TechNet topic describes System Access Control Lists in general:

- How Security Descriptors and Access Control Lists Work: https://technet.microsoft.com/en-us/library/cc781716(v=ws.10).aspx

To enable/disableTLS event logging in the System Event Log, see the following link:

- https://technet.microsoft.com/en-us/library/Dn786445.aspx#BKMK_HowToEnableSchannelEventLogging

Wevtutil is a system utility that performs many of the management functions related to system and audit logons including the following:

- configure local audit storage capacity
- configure audit rules (includes enable/disable event logging for optional logging)
- enumerate the log names
- configure Analytic and Debug logs as enabled (e.g. Microsoft-Windows-CodeIntegrity/Verbose)

See the following article for more info on Wevtutil: http://technet.microsoft.com/en-us/library/cc732848.aspx

To view audit logs, see the following link:

- Get-EventLog: http://technet.microsoft.com/en-us/library/hh849834.aspx

4 Managing TLS

4.1 Local Administrator Guidance

The cipher suites listed in the Security Target correlate with those available in the Windowsas follows:

Ciphersuitesprelisted in the Security Target		**Setting name for the cipher suites in Windows[1]**
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246		TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246		TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246		TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246		TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384

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=ws.10).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:

[1] See: Cipher Suites in Schannel: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.10).aspx

- 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.10).aspx

The configuration for elliptic curves is slightly different on Windows 10 and Server 2012 R2. By default, the secp521r1 curve is not enabled for either operating system. A reboot of the system is required after changing the cipher suite or elliptic curves configuration.

Server 2012 R2: 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. To enable this cipher suite with an elliptic curve, e.g. secp256r1, you use the SSL cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256. The difference is the final four characters which indicate the elliptic curve that is to be used where P256 equals secp256r1.

Windows 10: There is a SSL Cipher Suite Order list and a ECC Curve Order list displayed in the Local Policy Editor. Enable and order the desired cipher suites in the first list and enable/order the elliptic curves in the second. For example, to configure only TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite and secp256r1 curve, edit the first list to only include TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and the Curve order list to only include secp256r1 (or NistP256 as it is shown in the Local Policy Editor). Additional cipher suites and curves in each list will generate additional options in the client hello.

The reference identifier in Windows 10 and Windows Server 2012 R2 for TLS is the URL of the server. There is no configuration of the reference identifier.

The signature_algorithm set that is acceptable to the client (offered in the signature_algorithm extension during client hello) is configurable by editing the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010003. Remove the signature algorithm that should not be used. No additional algorithms other than the default set may be specified.

4.2 User Guidance

Users may choose using TLS with HTTPS by using https in the URL typed into the browser.

5 Managing Account Lockout Policy

5.1 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.

6 Managing Passwords and Password Policy

6.1 Local Administrator Guidance

The following TechNet topic describes how to configure the minimum password length policy:

- Net accounts: https://technet.microsoft.com/en-us/library/bb490698.aspx

The following TechNet topics describe how to configure password complexity policy:

- Passwords must meet complexity requirements: https://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx
- Apply or modify password policy: https://technet.microsoft.com/en-us/library/cc781633(v=ws.10).aspx

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

The Local Administrator may disable unauthenticated logon by configuring user accounts to have a password.The out of box experience requires that when user accounts are created a password is assigned to the account.

6.2 User Guidance

To change an account password do either of the following:

- (Windows 10 only) 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

7 Managing Certificates

7.1 Local Administrator Guidance

The following TechNet topic describes managing certificates (including the “Obtain a Certificate” sub-topic for requesting or enrolling certificates and the “Automate Certificate Management” sub-topic for managing certificate path validation):

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

The following TechNet topic describes how to delete a certificate:

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

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.

The administrator configures certificate templates for TLS client authentication as described in the following TechNet topics:

- Managing Certificate Templates:https://technet.microsoft.com/en-us/library/cc772457.aspx
- Cryptography (for configuring the algorithm that the issued certificate's key pair will support):https://technet.microsoft.com/en-us/library/cc770477.aspx

The administrator configures the correct algorithms for the given cipher suites according to the following table):

Cipher Suites (per Security Target)	**Selections in the certificate template**
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246	Provider Category = Key Storage Provider Algorithm Name = RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	Provider Category = Key Storage Provider Algorithm Name = ECDSA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	Provider Category = Key Storage Provider Algorithm Name = ECDSA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492	Provider Category = Key Storage Provider

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	Algorithm Name = ECDSA_P521

Windows 10 and Windows Server 2012 R2 automatically generate asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no configuration is necessary.

Windows 10 and Windows Server 2012 R2 automatically generate asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4,no configuration is necessary.

Windows 10 and Windows Server 2012 R2 automatically implement RSA-based key establishment schemes that meet SP-800-56B,no configuration is necessary.

Windows 10 and Windows Server 2012 R2 automatically implement elliptic curve-based key establishment schemes that meet SP-800-56A,no configuration is necessary.

7.2 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

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

The user obtains a client certificate for authentication by following the procedures in the following Technet topic:

- Obtain a Certificate: https://technet.microsoft.com/en-us/library/cc754246.aspx

8 Managing Screen Lock and Session Timeout

8.1 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

The inactivity timeout for remote sessions is configured by the administrator via Windows security policy. The relevant policy is “Set time limitfor active but idle Remote Desktop Services session” as described in the following TechNet topic:

- Session Time Limits: https://technet.microsoft.com/en-us/library/ee791741.aspx

8.2 User Guidance

To configure screen lock timeout:

- Windows 10: Go to Settings ->System ->Power & sleep -> Additional power settings -> Change when the computer sleeps
- Windows Server 2012R2: Control Panel -> Hardware -> Power Options -> Change when to turn off the display

The following describes how to configure screen savers:

- Windows 10: http://windows.microsoft.com/en-us/windows-10/getstarted-lock-screen
- Windows Server 2012R2: Control Panel -> Appearance -> Display -> Change screen saver

To manage notifications on the lock screen:

- Windows 10: Go to Settings ->System ->Notifications & actions

To initiate a screenlock:

- Click on the Start button, then on the user picture (upper left in Start Menu), and then click **Lock**
- **- or –** type Windows logo key + L

9 Managing Local Area Network

9.1 Local Administrator Guidance

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

10 Managing Bluetooth

10.1 Local AdministratorGuidance

The local administrator can enable and disable the Bluetooth radio in the Device Manager application by right-clicking the Bluetooth/<radio adapter> node (where <radio adapter> refers to the name of the Bluetooth radio adapterfor the computer) and selecting the Properties menu item to open the “<radio adapter> Properties” window. The local administrator then clicks the Driver tab In the “<radio adapter> Properties window and clicks the Enable or Disable button

No configuration is necessary to ensure the Bluetooth services provided before login are limited.

10.2 User Guidance

The following topic describes how to initiate and complete pairing with a Bluetooth device:

- Add a Bluetooth device to Surface devices: https://www.microsoft.com/surface/en-us/support/hardware-and-drivers/add-a-bluetooth-device?os=windows-10
- Add a Bluetooth device to all other hardware platforms: http://windows.microsoft.com/en-US/windows7/Add-a-Bluetooth-enabled-device-to-your-computer

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

11 Managing USB

11.1 Local Administrator Guidance

The local administrator disables 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 the Enable or Disable button.

12 Managing Updates

12.1 Local Administrator Guidance

For Windows 10, Windows Update is described in the following technet articles:

- Keep your PC up to date: http://windows.microsoft.com/en-us/windows/windows-update

The following steps shall be performed in order to check for updates for Windows 10:

- Open **Settings**
- Click **Update & Security**
- Under Windows Update, click **Check for updates**

The following steps shall be performed in order to check for updates for Windows Server 2012 R2:

- Open **Control Panel**
- Click **System and Security**
- Under **Windows Update**, click **Check for updates**

The local administrator configures autoamatic updates as described in the following TechNet topic:

- Configure Automatic Updates using Group Policy: https://technet.microsoft.com/en-us/library/dd939933.aspx

The following help topics describe how to check for updates to Windows Store installed applications on Windows 10:

- Check for updates for apps and games from Windows Store: http://windows.microsoft.com/en-us/windows-10/check-for-updates-for-apps-and-games-from-windows-store

Follow the same procedures on Windows Server 2012 R2 if Desktop Experience is configured:

- Desktop Experience Overview:https://technet.microsoft.com/en-us/library/dn609826.aspx

13 Managing the Firewall

13.1 Local Administrator Guidance

The following TechNet topic describes how the Windows Firewall is managed using PowerShell cmdlets (e.g. see Set-NetFirewallSetting):

- Network Security Cmdlets in Windows PowerShell: https://technet.microsoft.com/en-us/library/jj554906(v=wps.630).aspx

14 Managing Domains

14.1 Local Administrator Guidance

The following TechNet topic describes how to join a client computer to an Enterprise domain

- How to Join Your Computer to a Domain: https://technet.microsoft.com/en-us/library/bb456990.aspx

The name of the domain that is indicated for the Domain entry in step (2) should be provided by your IT administrator.

Choosing a domain is equivalent to choosing a Management Server.

15 Managing Time

15.1 Local Administrator Guidance

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

- Using the Set-Date Cmdlet: 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

16 Managing Wi-Fi

16.1 Local Administrator Guidance

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

17 Managing Remote Administration

17.1 Local Administrator Guidance

The following linksprovide information on how to use RDP to establish a trusted remote OS administration session:

- Remote Desktop Services Overview: https://technet.microsoft.com/en-us/library/hh831447.aspx
- Connect to another computer using Remote Desktop Connection: http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7

RDP session security is controlled by the RDP host in most cases. The following link provides information on how to require TLS for RDP sessions:

- Configure Server Authentication and Encryption Levels:https://technet.microsoft.com/en-us/library/cc770833.aspx

Note that in Windows Server 2012 R2 and Windows 10, TLS 1.2 will be negotiated using the above settings.

The following link provides information on configuring Session Time Limits for remote connections:

- Session Time Limits : https://technet.microsoft.com/en-us/library/cc753112.aspx

18 Managing Software Restriction Policies

18.1 Local Administrator Guidance

On Windows 10 Enterprise, Device Guard is used to manage Software Restriction Policies. See the link below for information on Device Guard:

Device Guard overview: https://technet.microsoft.com/en-us/library/dn986865(v=vs.10).aspx

On all other Windows editions, AppLocker is used to manage Software Restriction Policies. See the link below for information on AppLocker:

AppLocker Overview: https://technet.microsoft.com/en-us/library/hh831409.aspx

19 Managing Logon Banner

19.1 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

20 Managing Hibernation

20.1 Local Administrator Guidance

The following TechNet topic describes how to manage power configuration, including disabling the hibernate function:

- Powercfg Command-Line Options: https://technet.microsoft.com/en-us/library/cc748940(v=ws.10).aspx

21 Managing PIN Sign-in

21.1 User Guidance

To turn on username/PIN authentication for a local standard user account on Windows 10 perform the following steps:

1. Login to the local standard user account
2. Go to Settings -> Accounts -> Sign-in options
3. Set a PIN sign-in option
    - Requires entering your username password first
4. Sign out

22 Developing Applications

This section of the operational guidance is not related to the management functions that may be performed by the user roles.

Developers may use Microsoft Visual Studio 2015 for development of applications. The following is a link to documentation for Microsoft Visual Studio 2015:

- Visual Studio : https://www.visualstudio.com/en-us/visual-studio-homepage-vs.aspx

Applications developed in Microsoft Visual Studio 2015 will by default have the /GS flag set. The following is a link to documentation about the /GS flag in Microsoft Visual Studio 2015:

- /GS (Buffer Security Check) : https://msdn.microsoft.com/en-us/library/8dbf701c.aspx