# Microsoft Windows

# Common Criteria Evaluation

## Microsoft Windows 10 Fall Creators Update

## Microsoft Windows Server (Fall Creators Update)

# Common Criteria Supplemental Admin Guidance

| Document Information | |
|---|---|
| Version Number | 0.6 |
| Updated On | March 20, 2018 |

**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 10 (Fall Creators Update).

## 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 (Fall Creators Update) (32-bit version)
- Microsoft Windows 10 Pro Edition (Fall Creators Update) (64-bit versions)
- Microsoft Windows 10 Enterprise Edition (Fall Creators Update) (64-bit versions)
- Microsoft Windows 10 S Edition (Fall Creators Update)
- Microsoft Windows Server Standard Core, version 1709
- Microsoft Windows Server Datacenter Core, version 1709

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

- Microsoft Surface Book 2
- Microsoft Surface Laptop
- Dell Latitude 5290
- Dell PowerEdge R740
- Microsoft Windows Server Hyper-V
- Microsoft Windows Server 2016 Hyper-V

## 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 topic has procedures to download installation media as an ISO file for installation, create bootable media using the ISO file, and to install the operating system for Windows 10 Home and Pro editions:

- Download Windows 10: https://www.microsoft.com/en-us/software-download/windows10[1]

The following topic has procedures to download Windows Server 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:

- Windows Server: https://www.microsoft.com/Licensing/servicecenter/default.aspx

Installation media for Enterprise editions are obtained through Volume Licensing.

#### *1.2.1.1 Managing User Roles*

The evaluated configuration includes two user roles:

- 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 require local 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

[1] This link applies only to Pro and Home editions.

The operational guidance includes sections for “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 Enrolling with a MDM*

The following links provide guidance on enrolling Windows devices for device management:

- MDM enrollment of Windows-based devices: https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices

MDMs may also have pre-requisites for enrollment, for example trust of the MDM’s certificate. Guidance for MDM pre-requesites are out of scope of this documentation. IT Administrators should consult the MDM documentation to make sure that pre-requisites are understood and met before enrollment is performed.

Windows Server can not be enrolled with an MDM.

#### *1.2.1.3 Setup Requirements*

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

- Windows 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 document labeled as “Administrator Guidance”, or set the device up for IT administration. For Windows 10 IT administration is enrolling the device for device management in order to receive MDM policies. For Windows Server IT administration is joining the device to a Windows domain in order to received domain group policy.
- Administators must utilize the guidance included in this document to administer the device.
- Available security updates shall be applied. Available updates can be found at: https://support.microsoft.com/en-us/help/4043454/windows-10-windows-server-update-history.

##### 1.2.1.3.1 Security Policy Settings

The following security policies must be applied by an administrator after completing the OOBE in 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 Templates\Windows Components\Credentials User Interface\Do not display the password reveal button | Enabled |

These two policies may be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for FIPS: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-cryptography. The following link describes the MDM policy for password reveal: CredentialsUI/DisablePasswordReveal.

The above security policy settings may also be configured using Group Policy Editor (gpedit.msc) or Local Security Policy Editor (secpol.msc). These tools are not available on Windows Home Edition. For Windows Home Edition and Windows Server enable the above two policies by using the following PowerShell commands:

Enable “System cryptography: Use FIPS 140…”:

```
Set-ItemProperty -Path Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\fipsAlgorithmPolicy -Name Enabled -Value "1"
```

Enable “Do not display the password reveal button”:

```
$pathKey = "Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredUI"
If (!(Test-Path -Path $pathKey)){
   New-Item -Path Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows -Name CredUI -ItemType Folder
}
New-ItemProperty -Path $pathKey -Name DisablePasswordReveal -Value "1" -PropertyType DWORD -Force
```

#### 1.2.1.3.2 Using Group Policy Editor Remotely

Group Policy Editor may be used to remotely administrate policy on a machine. This is especially useful on Windows Server.

1. Start -> Run -> mmc
2. File -> Add/Remove Snap-in
3. Under the Standalone tab, click Add...
4. Choose Group Policy Object Editor
5. In the following wizard, click the Browse button
6. Click the "Computers" tab, select the Another computer radial button, and type the name or Browse to the remote computer
7. Click OK, then Finish, then Close, and finally OK

#### 1.2.1.3.3 Other Settings

The following security settings must also be applied to fulfill the security objectives for the evaluated configuration:

- Cipher suite selection must be configured according to Section 4 Managing TLS
- When Windows is configured to use TLS 1.2, SHA1 algorithms should be prioitized at the bottom of the algorithm negotiation list as described in Section 4 Managing TLS.
- Complex passwords  must be configured as described inSection 8 Managing Passwords
- RSA machine certificates must be configured according to Section 9 Managing Certificates to use a minimum 2048 bit key length
- Session locking must be enabled according to section 10 Locking a Device
- Hibernation must be disabled according to section 22 Managing Hibernation

#### *1.2.1.4 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 options are configured to enable kernel 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.

### 1.2.2 Windows 10 S

For configuring Windows 10 S edition, the PowerShell functionality is not accessible for use of PowerShell cmdlets nor is the command shell for executing command line utilities. Configuration alternatives may be suggested for Windows S edition when a PowerShell option is provided. Command line utilities must be executed on Windows S edition in the **Create new task** window that is started by selecting **Run new task** in the **File** menu for the Task Manager (taskmgr.exe). Note by default the task is started without administrator privileges causing commands that administrator privileges to fail – to run a command with administrator privileges check the **Create this task with administrator privileges** checkbox.

Security policies as described in the Security Policy Settings section above are applied to Windows 10 S using an MDM.

Administrative guidance indicating use of an MDM are applicable to Windows S edition unless otherwise noted.

# 2 Management Functions

The following table maps management functions to sections in this document. As indicated by the "Administrator" and "User" columns, some management functions have activities that may only be performed by an 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 | Administrator | User |
|---|---|---|---|---|
| 1 | enable/disable screen lock | 10 | √ | √ |
| 2 | configure screen lock inactivity timeout | 10 | √ | √ |
| 3 | configure local audit storage capacity | 3 | √ | |
| 4 | configure minimum password length | 8 | √ | |
| 5 | ~~configure minimum number of special characters in password~~ | - | | |
| 6 | ~~configure minimum number of numeric characters in password~~ | - | | |
| 7 | ~~configure minimum number of uppercase characters in password~~ | - | | |
| 8 | ~~configure minimum number of lowercase characters in password~~ | - | | |
| 9 | configure remote connection inactivity timeout | 10 | √ | |
| 10 | ~~enable/disable unauthenticated logon~~ | - | | |
| 11 | configure lockout policy for unsuccessful authentication attempts through [***timeouts between attempts, limiting number of attempts during a time period***] | 5 | √ | |
| 12 | configure host-based firewall | 15 | √ | |
| 13 | configure name/address of directory server to bind with | 16<br>No Windows 10 S Support | √ | |
| 14 | configure name/address of remote management server from which to receive management settings | 1.2.1.2, 16 | √ | |
| 15 | ~~configure name/address of audit/logging server to which to send audit/logging records~~ | - | | |
| 16 | configure audit rules | 3 | √ | |
| 17 | configure name/address of network timeserver | 17 | √ | |
| 18 | enable/disable automatic software update | 14 | √ | |
| 19 | configure WiFi interface | 18 | √ | |

| | | | | |
|---|---|---|---|---|
| 20 | enable/disable Bluetooth interface | 12 | √ | |
| 21 | configure USB interfaces | 13 | √ | |
| 22 | enable/disable [**local area network interface**] | 11 | √ | |

# 3 Managing Audits

## 3.1 Audit Events

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

| **Description** | **Id** |
|---|---|
| Start-up and shut-down of the audit functions | Start-up: **4608**<br>Shut-down: **1100** |
| Authentication events (Success/Failure) | Success: **4624**<br>Failure: **4625** |
| Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes) | WRITE_DAC : **4670**<br>All other object access writes : **4656** |
| Privilege or role escalation events (Success/Failure) | Success: **4673**<br>Failure: **4674** |
| File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions) | **4656** |
| User and Group management events (Successful and unsuccessful add, delete, modify, disable) | add user: **4720**<br>add user to group: **4732**<br>delete user: **4726**<br>delete user from group: **4733**<br>add group: **4731**<br>delete group: **4734**<br>modify group: **4735**<br>modify user account: **4738**<br>disable user: **4725** |
| Lock and unlock a user account | Lock: **4740**<br>Unlock: **4767** |
| Audit and log data access events (Success/Failure) | Success, Failure: **4673** |

| | |
|---|---|
| Cryptographic verification of software (Success/Failure) | Failure: **3**<br>Success: **2** |
| Program initiations (Success/Failure e.g. due to software restriction policy) | Success: **3038** (Device Guard), **8020** (AppLocker)<br>Failure: **3077** (Device Guard) , **8022** (AppLocker) |
| System reboot, restart, and shutdown events (Success/Failure), | Start-up: **4608**<br>Shut-down: **1100** |
| Kernel module loading and unloading events (Success/Failure), | Success: **3038** (Other kernel modules), **Windows Boot Configuration Log** (Boot kernel module loading)<br>Failure: **3004** (Other kernel modules), **Recovery Screen** (Boot kernel module loading) |
| Administrator or root-level access events (Success/Failure), | Success: **4624**<br>Failure: **4625** |

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

**Note:** The fields in the following table refer to the hierarchical field names used in Event Viewer event data on the **Details** tab when the **Friendly View** radio button is selected. The field names also correspond to the node names in XML files provided as evidence. The **Message** values correspond to the message displayed in the **General** tab.

| Id | Log location | Message | Fields |
|---|---|---|---|
| **2** | **Windows Logs->Setup** | Package was successfully changed to the Installed state | **System**->**TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Security[UserID]**: <Subject identifier ><br>**System->Level**: <Outcome as Success or Failure> |
| **3** | **Windows Logs->Setup** | Windows update could not be installed because … “The data is invalid” | **System**->**TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Security[UserID]**: <Subject identifier ><br>**System->Level**: <Outcome as Success or Failure> |
| **1100** | **Windows Logs->Security**<br>Subcategory: Security State Change | The event logging service has shut down | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**N/A**: <Subject identifier> |

| | | | |
|---|---|---|---|
| **3004** | **Application and Services Logs->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. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Level**: <Outcome as Success or Failure><br>**System->Security[UserID]**: <Subject identifier> |
| **3038** | **Application and Services Logs->Microsoft->Windows->CodeIntegrity->Verbose** | Code Integrity started validaging image header of <kernel module pathname> file | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Level**: <Outcome as Success or Failure><br>**System->Security[UserID]**: <Subject identifier> |
| **3077** | **Application and Services Logs->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. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Level**: <Outcome as Success or Failure><br>**System->Security[UserID]**: <Subject identifier> |
| **4608** | **Windows Logs->Security**<br><br>Subcategory: Security State Change | Startup of audit functions | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**N/A**: <Subject identifier> |
| **4624** | **Windows Logs->Security**<br><br>Subcategory: Logon | An account was successfully logged on. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->TargetUserSid**: <Subject identifier> |
| **4625** | **Windows Logs->Security**<br><br>Subcategory: Logon | An account failed to log on. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->TargetUserSid**: <Subject identifier> |
| **4656** | **Windows Logs->Security**<br><br>Subcategory: Handle Manipulation | A handle to an object was requested. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4670** | **Windows Logs->Security**<br><br>Subcategory: Policy Change | Permissions on an object were changed. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4673** | **Windows Logs->Security** | A privileged service was called. | **System->TimeCreated**[**SystemTime**]: <Date and time of event> |

| | | | |
|---|---|---|---|
| | Subcategory: Sensitive Privilege Use | | **System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4674** | **Windows Logs->Security**<br><br>Subcategory: Sensitive Privilege Use | An operation was attempted on a privileged object. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4720** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A user account was created. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4725** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A user account was disabled. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4726** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A user account was deleted. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4731** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A security-enabled local group was created. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4732** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A member was added to a security-enabled group. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4733** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A member was removed from a security-enabled group. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |

| | | | |
|---|---|---|---|
| **4734** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A security-enabled local group was deleted. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4735** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A security-enabled local group was changed. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4738** | **Windows Logs->Security**<br><br>Subcategory: User Account Management | A user account was changed | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4740** | **Windows Logs->Security**<br><br>Subcategory: Account Lockout | A user account was locked out. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **4767** | **Windows Logs->Security**<br><br>Subcategory: Account Lockout | A user account was unlocked. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Task**: <Type of event><br>**System->Keywords**: <Outcome as Success or Failure><br>**EventData->SubjectUserSid**: <Subject identifier> |
| **8020** | **Application and Services Logs->Microsoft->Windows->AppLocker->Packaged app-Execution** | <Packaged app name> was allowed to run. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Level**: <Outcome as Success or Failure><br>**System->Security[UserID]**: <Subject identifier> |
| **8022** | **Application and Services Logs->Microsoft->Windows->AppLocker->Packaged app-Execution** | <Packaged app name> was prevented from running. | **System->TimeCreated**[**SystemTime**]: <Date and time of event><br>**System->Provider[Name]**: <Type of event><br>**System->Level**: <Outcome as Success or Failure><br>**System->Security[UserID]**: <Subject identifier> |

## 3.2 Managing Audit Policy

### 3.2.1 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 failure in 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

The Local Security Policy (secpol.msc) utility is used as an alternative to the auditpol utility for managing Security audits on Windows 10 S edition. The following TechNet link describes how to use the Local Security Policy utility: Administer Security Policy Settings.

In addition to enabling audit policy as noted above, each registry key or file 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 the file object, click **Security**, click **Advanced**, and click **Auditing**. On Windows Server the File Explorer is not locally available but can be used remotely. PowerShell may also be used to set the SACL on the file object.

- Get-Acl: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl?view=powershell-6
- Set-Acl: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-6

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

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 using PowerShell, see the following link:

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

For Windows S edition audit logs are reviewed using the Event Viewer application, see the following link:

- Event Viewer How To…: https://technet.microsoft.com/en-us/library/cc749408(v=ws.11).aspx

# 4 Managing TLS

## 4.1 Administrator Guidance

### 4.1.1 Cipher Suite Selection

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

| **Cipher suites prelisted in the Security Target** | **Setting name for the cipher suites in Windows[2]** |
|---|---|
| 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<br>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384<br>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 |

[2] See: TLS Cipher Suites in Windows 10 1709: https://msdn.microsoft.com/en-us/library/windows/desktop/mt813794(v=vs.85).aspx

TLS cipher suite priority and restricting use of certain cryptographic algorithms may be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for TLS cipher suites: Cryptography/TLSCipherSuites.

The Group Policy Editor and the Local Secuity Policy Editor may also be used as described in the following MSDN articles to allow the administrator to modify the set of TLS cipher suites for priority and availability:

- Prioritizing Schannel Cipher Suites: https://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

Hashes in the TLS protocol are configured in association with cipher suite selection.

The configuration for elliptic curves uses a SSL Cipher Suite Order list and a ECC Curve Order list displayed in the Group Policy Editor and the Local Secuity 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 policy editor). Additional cipher suites and curves in each list will generate additional options in the client hello.By default, the secp521r1 curve is not enabled. A reboot of the system is required after changing the cipher suite or elliptic curves configuration.

Manage TLS cipher suites and elliptic curves using the following PowerShell cmdlets:

- Enable-TlsCipherSuite
- Disable-TlsCipherSuite
- Enable-TlsEccCurve
- Disable-TlsEccCurve

### 4.1.2 Certificate Name Comparison

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 reference identifiers for TLS are the DNS name or IP address of the remote server, which is compared against the DNS name as the presented identifier in either the Subject Alternative Name (SAN) or the Subject Name of the certificate. There is no configuration of the reference identifiers.

### 4.1.3 Root Certificates

The device 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 link provides information on how to import root certificates using PowerShell:

- Import-Certificate: http://technet.microsoft.com/en-us/library/cc754841.aspx

The trust relationships may also be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for trusted root certificates: RootCATrustedCertificates CSP.

### 4.1.4 Managing Signature Algorithms

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.

For Windows 10 S edition the registry is edited remotely as described by the following TechNet topic: Connect to the Registry.

## 4.2 User Guidance

### 4.2.1 Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S

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

# 5 Managing Account Lockout Policy

## 5.1 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 Smart Card Logon

Smartcard logon is supported on Windows domain-joined devices. IT administrators must enable an account for smartcard logon and issue a smartcard to a user.

# 7 Managing Windows Hello - Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S

## 7.1 Managing Biometric Authentication

### 7.1.1 User Guidance

To enable Windows Hello and add authentication mechanisms other than password:

1. Login to the user account
2. Go to **Settings -> Accounts -> Sign-in options**
3. Review the Windows Hello options and select either **Fingerprint** or **Face Recognition**
4. Follow the instructions in the Windows Hello setup wizard
5. Sign out

## 7.2 Managing PIN Authentication

### 7.2.1 Administrator Guidance

To enable using a PIN in place of passwords on domain-joined devices, the following security policy must be enabled using the Group Policy Editor (gpedit.msc): Administrative Templates\System\Logon\Turn on convenience PIN sign-in.

### 7.2.2 User Guidance

To enable Pin in place of passwords:

1. Login to the user account
2. Go to **Settings -> Accounts -> Sign-in options**
3. Under the **PIN** heading tap the **Add** button and choose a new PIN value in the **Set a PIN** window
    - Requires entering your username password to confirm the operation
4. Sign out

Note the PIN sign-in options user interface is not displayed when the device is logged on remotely via Remote Desktop Protocol or when it is hosted in a Hyper-V virtual machine in Enhanced Session mode.

# 8 Managing Passwords and Password Policy

## 8.1 Administrator Guidance

Password policy may be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for passwords (see “DeviceLock Policies”): Policy CSP.

The Group Policy Editor or Local Security Policy Editor may also be used to set password security policies on Windows 10 Enterprise, Windows 10 Pro, Windows 10 S and Windows Server. The following TechNet topic provides an overview of password security policies and links to information for each security policy setting:

- Password Policy: https://technet.microsoft.com/en-us/library/hh994572(v=ws.10).aspx

Enable password policies using the following utilities on Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home and Windows Server:

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

The Administrator may disable unauthenticated logon by configuring user accounts to have a password. The OOBE requires user accounts to be created with a password.

# 9 Managing Certificates

## 9.1 Administrator Guidance

### 9.1.1 Client Certificates

Certificates may be managed by the IT Administrator using a MDM. See the MDM solution documentation for detailed management actions. The following link describes the MDM policy for client certificate management: ClientCertificateInstall CSP.

The following TechNet topic also 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

### 9.1.2 Root Certificates

The device comes preloaded with root certificates for various Certificate Authorities.

Certificate trust relationships may be managed by the IT Administrator using a MDM. See the MDM solution documentation for detailed management actions. The following link describes the MDM policy for trusted root certificates: RootCATrustedCertificates CSP. The following link describes the MDM policy to delete client certificates: ClientCertificateInstall CSP.

The following TechNet topic also describes how to manage trusted roots with the Group Policy Editor or Local Security Policy Editor:

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

The remove-item PowerShell cmdlet may be used to delete certificates and wipe the private keys associated with the certificate. The following TechNet topic describes how to use the remove-item cmdlet:

- Using the Remove-Item Cmdlet: https://technet.microsoft.com/en-us/library/ee176938.aspx

The following TechNet topic describes how to delete a certificate with the Group Policy Editor or Local Security Policy Editor:

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

### 9.1.3 Certificate Validation

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.

#### *9.1.3.1 HTTPS - Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S*

The administrator configures certificate validation for HTTPS for Internet Explorer using the checkbox options in the **Security** category that are shown in the **Settings** panel on the **Advanced** tab for the **Internet Properties** window. The **Internet Properties** is opened by the **Internet Options** icon in the **Control Panel** or from the configuration settings menu in Internet Explorer. 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 HTTPS for Microsoft Edge. If the Web address does not match the certificate subject field, then the user is warned of a mismatch.

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

#### *9.1.3.2 Code Signing*

The administrator cannot configure certificate validation for code signing purposes.

### 9.1.4 Certificate Enrollment

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 administrator.

The IT 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
- PowerShell commands for configuring the algorithm that the issued certificate's key pair will support: https://docs.microsoft.com/en-us/powershell/module/tls/?view=win10-ps

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 | Provider Category = Key Storage Provider<br>Algorithm Name = RSA |

| | |
|---|---|
| TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246<br>TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246<br>TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246<br>TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246<br>TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246<br>TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 | |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492<br>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 | Provider Category = Key Storage Provider<br>Algorithm Name = ECDSA_P256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 | Provider Category = Key Storage Provider<br>Algorithm Name = ECDSA_P384 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 | Provider Category = Key Storage Provider<br>Algorithm Name = ECDSA_P521 |

Windows automatically generates asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no configuration is necessary.

Windows automatically generates asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4, no configuration is necessary.

Windows automatically implements RSA-based key establishment schemes that meet SP-800-56B, no configuration is necessary.

Windows automatically implements elliptic curve-based key establishment schemes that meet SP-800-56A, no configuration is necessary.

Windows automatically generates random bits according to SP-800-90A, no configuration is necessary.

## 9.2 User Certificates

Certificates may be imported or obtained for client authentication by the IT Administrator using a MDM. See the MDM solution documentation for detailed actions. The following link describes the MDM policy for client certificate management: ClientCertificateInstall CSP.

### 9.2.1 User Guidance

#### *9.2.1.1 Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows Server*

The following link describes how to import a certificate and private key from a PFX file using PowerShell:

- import-pfxcertificate: https://docs.microsoft.com/en-us/powershell/module/pkiclient/import-certificate?view=win10-ps

The following link describes how to export a certificate and private key using PowerShell:

- export-pfxcertificate: https://docs.microsoft.com/en-us/powershell/module/pkiclient/export-pfxcertificate?view=win10-ps

#### *9.2.1.2 Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S*

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

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

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

# 10 Managing Screen Lock and Session Timeout

## 10.1 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

Screen lock and session timeout policy may also be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed actions. The following links describe the MDM policy for managing screen lock and session timeout policy:

- Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, Windows 10 S: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock

## 10.2 User Guidance

The following links provide indofrmation on registry settings which may be used to configure screenlock:

- ScreenSaveActive: https://technet.microsoft.com/en-us/library/cc978620.aspx
- ScreenSaverIsSecure: https://technet.microsoft.com/en-us/library/cc959646.aspx
- ScreenSaveTimeout: https://technet.microsoft.com/en-us/library/cc978621.aspx

### 10.2.1 Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S

To configure screen lock timeout:

- Go to **Settings -> System ->Power & sleep -> Additional power settings -> Change when the computer sleeps**

The following describes how to configure screen savers:

- http://windows.microsoft.com/en-us/windows-10/getstarted-lock-screen

To manage notifications on the lock screen:

- 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

# 11 Managing Local Area Network

## 11.1 Administrator Guidance

Enable/disable the wireless and local area network adapters: https://technet.microsoft.com/en-us/library/cc771762(v=ws.10).aspx

Network connections may be enabled/disabled using PowerShell. The following links provide information on how to enable/disable network connections with PowerShell:

- Disable-NetAdapter: https://docs.microsoft.com/en-us/powershell/module/netadapter/disable-netadapter?view=win10-ps
- Enable-NetAdapter: https://docs.microsoft.com/en-us/powershell/module/netadapter/enable-netadapter?view=win10-ps

The wireless network may also be enabled/disabled by the IT Administrator using a MDM. See the MDM solution documentation for detailed actions. The following link describes the MDM policy for managing wireless (see “WiFi policies”): Policy CSP.

# 12 Managing Bluetooth

## 12.1 Administrator Guidance

The 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 adapter for the computer) and selecting the **Properties** menu item to open the **<radio adapter> Properties** window. The administrator then clicks the **Driver** tab In the **<radio adapter> Properties** window and clicks the **Enable** or **Disable** button.

The following link provides the information on how to disable Bluetooth using PowerShell:

- Disable Bluetooth in Windows 10: https://blogs.technet.microsoft.com/jeff_stokes/2017/03/15/disable-bluetooth-in-windows-10/

The Bluetooth radio may also be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for enabling or disabling the Bluetooth radio: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-connectivity#connectivity-allowbluetooth[3].

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

### 12.2 User Guidance - Windows 10 Enterprise, Windows 10 Pro, Windows 10 Home, and Windows 10 S

To initiate and complete pairing with a Bluetooth device go to **Settings -> Devices -> Bluetooth & other devices**, tap **Add Bluetooth or other device** and then tap **Bluetooth** in the **Add a device** window to discover nearby Bluetooth devices available for pairing. Tap the desired Bluetooth device in the listing of discovered Bluetooth devices to initiate and complete pairing.

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

## 13 Managing USB

### 13.1 Administrator Guidance

The administrator disables USB ports 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 administrator then clicks the **Driver** tab In the **USB Root Hub Properties** window and clicks the **Enable** or **Disable** button.

USB controllers may be disabled/enabled with PowerShell. The following are links to PowerShell cmdlets that may be used to disable USB controllers:

- Get-PnpDevice: https://docs.microsoft.com/en-us/powershell/module/pnpdevice/get-pnpdevice?view=win10-ps
- Disable-PnpDevice: https://docs.microsoft.com/en-us/powershell/module/pnpdevice/disable-pnpdevice?view=win10-ps
- Enable-PnpDevice: https://docs.microsoft.com/en-us/powershell/module/pnpdevice/enable-pnpdevice?view=win10-ps

## 14 Managing Updates

### 14.1 Administrator Guidance

Windows Update is described in the following TechNet articles:

[3] This policy is not supported by Windows Home edition.

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

To check for updates go to **Settings -> Update & security** and then click the **Check for updates** button.

Windows Update may be configured to use enterprise Windows Server Update Services (WSUS) rather the default Microsoft Update. Configuring WSUS is outside the scope of this document.

The IT administrator may configure Automatic Updates or Windows Update for WSUS using the MDM. See the MDM solution documentation for detailed actions. The following link describes the MDM policy for managing updates: Policy CSP - Update.

The configuration may also be performed using domain group policy on Windows 10 Enterprise, Windows 10 Pro, Windows 10 S and Windows Server:

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

### 14.2 Windows Server

The following link describes how to check for Windows Updates on Windows Server using the SCONFIG utility, see the Windows Update settings section:

- Configure a Server Core installation of Windows Server 2016 or Windows Server, version 1709, with Sconfig.cmd: https://docs.microsoft.com/en-us/windows-server/get-started/sconfig-on-ws2016

### 14.3 User Guidance

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

- Check for updates for apps and games from Windows Store: https://support.microsoft.com/en-us/help/4026259/microsoft-store-check-updates-for-apps-and-games

## 15 Managing the Firewall

### 15.1 Administrator Guidance

The following TechNet topic describes how the Windows Firewall is managed using PowerShell cmdlets:

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

For Windows 10 S edition, click the **Windows Firewall** link in **Settings -> Network & Internet -> Status** to manage the Windows Firewall.

# 16 Managing Domains

## 16.1 Administrator Guidance

The following TechNet topic describes how to join a client computer to an Active Directory domain:

- How to Join Your Computer to a Domain: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain

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

The following link describes how to join a computer to a domain using PowerShell:

- Add-Computer: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/add-computer?view=powershell-5.1

Choosing a domain is equivalent to choosing a Management Server.

# 17 Managing Time

## 17.1 Administrator Guidance

### 17.1.1 Managing Date and Time

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

On Windows S edition the administrator sets the time in the **Control Panel** by opening the **Date and Time** window**,** and then pressing the **Change date and time…** button to open the **Date and Time Settings** window.

### 17.1.2 Managing the Time Service

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

# 18 Managing Wi-Fi

## 18.1 Administrator Guidance

The wireless network adapter is enabled or disabled in **Settings -> Network & Internet -> Status** by clicking the **Change adapter options** link to open the **Network Connections** window. In the **Network Connections** window select the Wi-Fi adapter and click the **Disable this network device** or **Enable this network device** button.

See the Manage Local Area Network section for information on managing network connections with PowerShell.

Wi-Fi may be configured by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for Wi-Fi policies: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-wifi.[4]

# 19 Managing Remote Administration

## 19.1 Administrator Guidance

Windows may be managed remotely by the IT Administrator using a MDM. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policies: https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference.

Windows may be managed remotely by the IT Administrator using domain group policy. The following link describes Managing Group Policy:

- Managing Group Policy: https://technet.microsoft.com/en-us/library/cc978280.aspx

The following links provide 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
- Microsoft Remote Desktop Clients: https://technet.microsoft.com/en-us/library/dn473009(v=ws.11).aspx

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

[4] This policy is not supported by Windows Home edition.

Note that 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

Windows may also be remotely managed using Powershell Remoting. PowerShell Remoting must be performed over a HTTPS connection. The following link provides information about on PowerShell Remoting:

PowerShell Remoting Security Considerations: https://docs.microsoft.com/en-US/powershell/scripting/setup/winrmsecurity?view=powershell-6

# 20 Managing Software Restriction Policies

## 20.1 Administrator Guidance

Device Guard is used to manage Software Restriction Policies. See the link below for information on Device Guard:

- Administer Software Restriction Policies: https://technet.microsoft.com/en-us/library/hh994606(v=ws.11).aspx

The following sample PowerShell script demonstrates a Device Guard policy to deny executing the Microsoft Edge browser application:

```
# By default no binaries are allowed to run so we need to allow most Windows binaries to run first.
# This will not allow unsigned binaries to execute.
# Add the set of signed binaries in "Program Files" and "Windows" folders and allow them to execute.
New-CIPolicy -Level PcaCertificate -UserPEs -ScanPath 'C:\Program Files' -FilePath allowProgramFiles.xml
New-CIPolicy -Level PcaCertificate -UserPEs -ScanPath C:\Windows -FilePath allowWindows.xml

# deny the Microsoft Edge app (which would otherwise be whitelisted by the above rule)
New-CIPolicy -Level FileName -UserPEs -Deny -ScanPath C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe -FilePath denyEdge.xml

# enforce the rules
Set-RuleOption -Delete 3 -FilePath allowProgramFiles.xml
Set-RuleOption -Delete 3 -FilePath allowWindows.xml
Set-RuleOption -Delete 3 -FilePath denyEdge.xml

#merge the three policy files and deploy the policy
```

```
Merge-CIPolicy -PolicyPaths '.\denyEdge.xml','.\allowWindows.xml','allowProgramFiles.xml' -OutputFilePath mergedPolicy.xml
convertFrom-CIPolicy mergedPolicy.xml mergedPolicy.bin
copy mergedPolicy.bin c:\windows\system32\codeintegrity\sipolicy.p7b
```

AppLocker may also be 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

Applocker is only supported in Windows 10 Enterprise edition and Windows Server. All editions, except, Enterprise, should use Device Guard to manage Software Restriction Policies.

# 21 Managing Logon Banner

## 21.1 Administrator Guidance

The following TechNet topics also describe how to configure a message to users attempting to logon with the Group Policy Editor or Local Security Policy Editor:

- Interactive logon: Message title for users attempting to log on: https://technet.microsoft.com/en-us/library/jj852182(v=ws.11).aspx
- Interactive logon: Message text for users attempting to log on: https://technet.microsoft.com/en-us/library/jj852199(v=ws.11).aspx

The message to users may also be configured by the IT administrator using a MDM for Windows 10 Enterprise, Pro and S editions. See the MDM solution documentation for detailed configuration actions. The following link describes the MDM policy for managing the welcome message: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-localpoliciessecurityoptions#localpoliciessecurityoptions-interactivelogon-displayuserinformationwhenthesessionislocked.

# 22 Managing Hibernation

## 22.1 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

# 23 Developing Applications

This section of the operational guidance is provided for application developers and is not related to the management functions that may be performed by the administrator or user roles described in the other sections of this document.

Developers may use Microsoft Visual Studio 2017 for development of applications. The following is a link to documentation for Microsoft Visual Studio 2017:

- Visual Studio : https://docs.microsoft.com/en-us/visualstudio/ide/visual-studio-ide

Applications developed in Microsoft Visual Studio 2017 will by default have the /GS flag set. The following is a link to documentation about the /GS flag in Microsoft Visual Studio:

- /GS (Buffer Security Check) : https://docs.microsoft.com/en-us/cpp/build/reference/gs-buffer-security-check