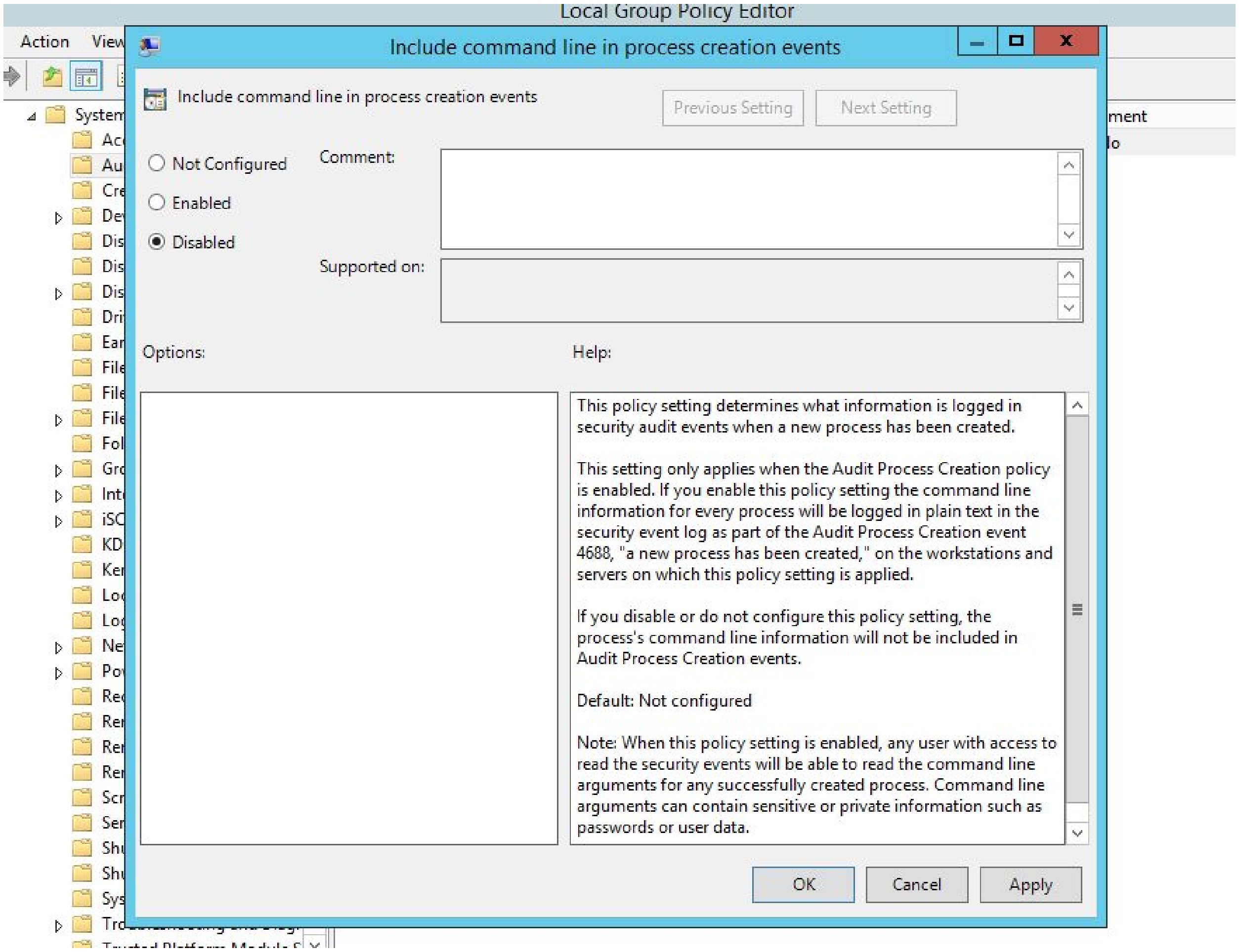
Final Project: *System Hardening*

Assignment Submission

Name: Van Linh Ha (116592171), Winston Lam (156576175), Jackson Lui (014713150), Tirth Patel (015790157)

Figure 1.1 Include Command Line in process creation events



Include command line in process creation events

○ Not Configured

○ Enabled

● Disabled

This policy setting determines what information is logged in security audit events when a new process has been created.

This setting only applies when the Audit Process Creation policy is enabled. If you enable this policy setting the command line information for every process will be logged in plain text in the security event log as part of the Audit Process Creation event 4688, "a new process has been created," on the workstations and servers on which this policy setting is applied.

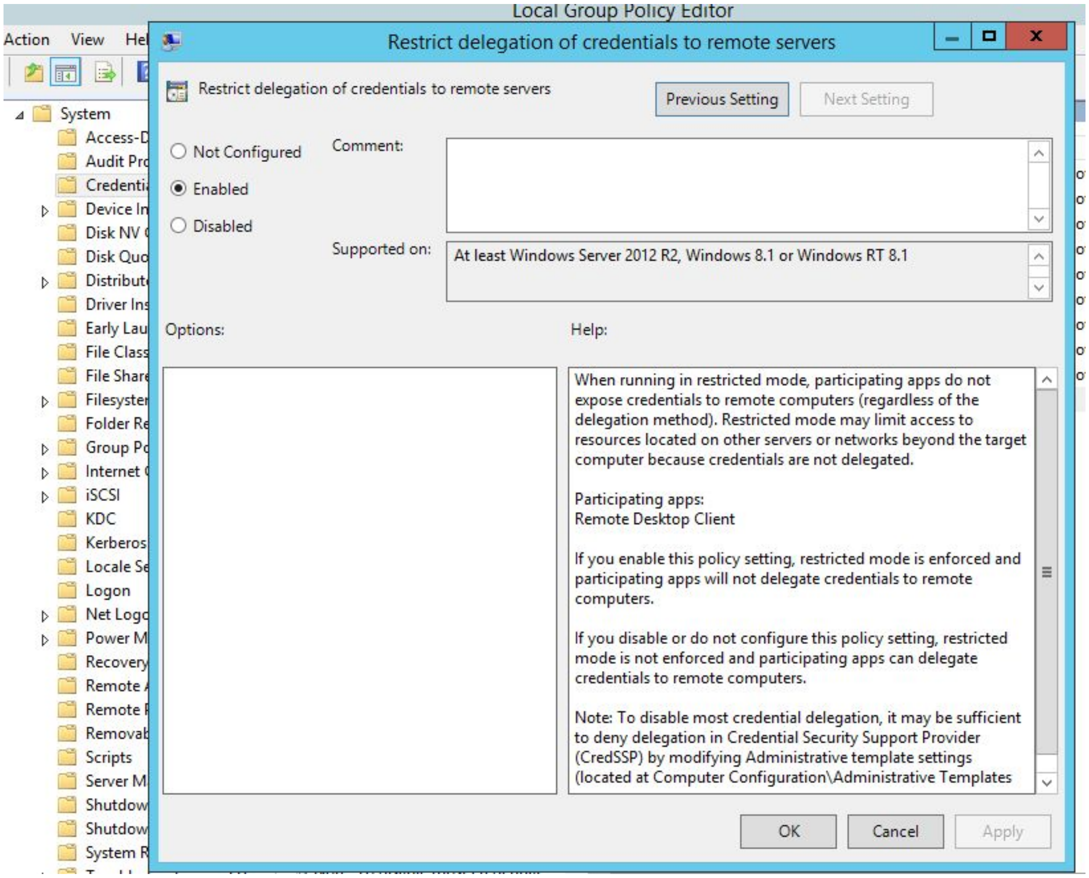
If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

Default: Not configured

Note: When this policy setting is enabled, any user with access to read the security events will be able to read the command line arguments for any successfully created process. Command line arguments can contain sensitive or private information such as passwords or user data.

Under this policy setting, it controls what kind of information is logged within the security audit events when a new process has been created. In Figure 1.1, Windows Server 2012 disabled this option.

Figure 1.2 – Restrict Delegation of credentials to remote servers



Restrict delegation of credentials to remote servers

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Help:

When running in restricted mode, participating apps do not expose credentials to remote computers (regardless of the delegation method). Restricted mode may limit access to resources located on other servers or networks beyond the target computer because credentials are not delegated.

Participating apps:
Remote Desktop Client

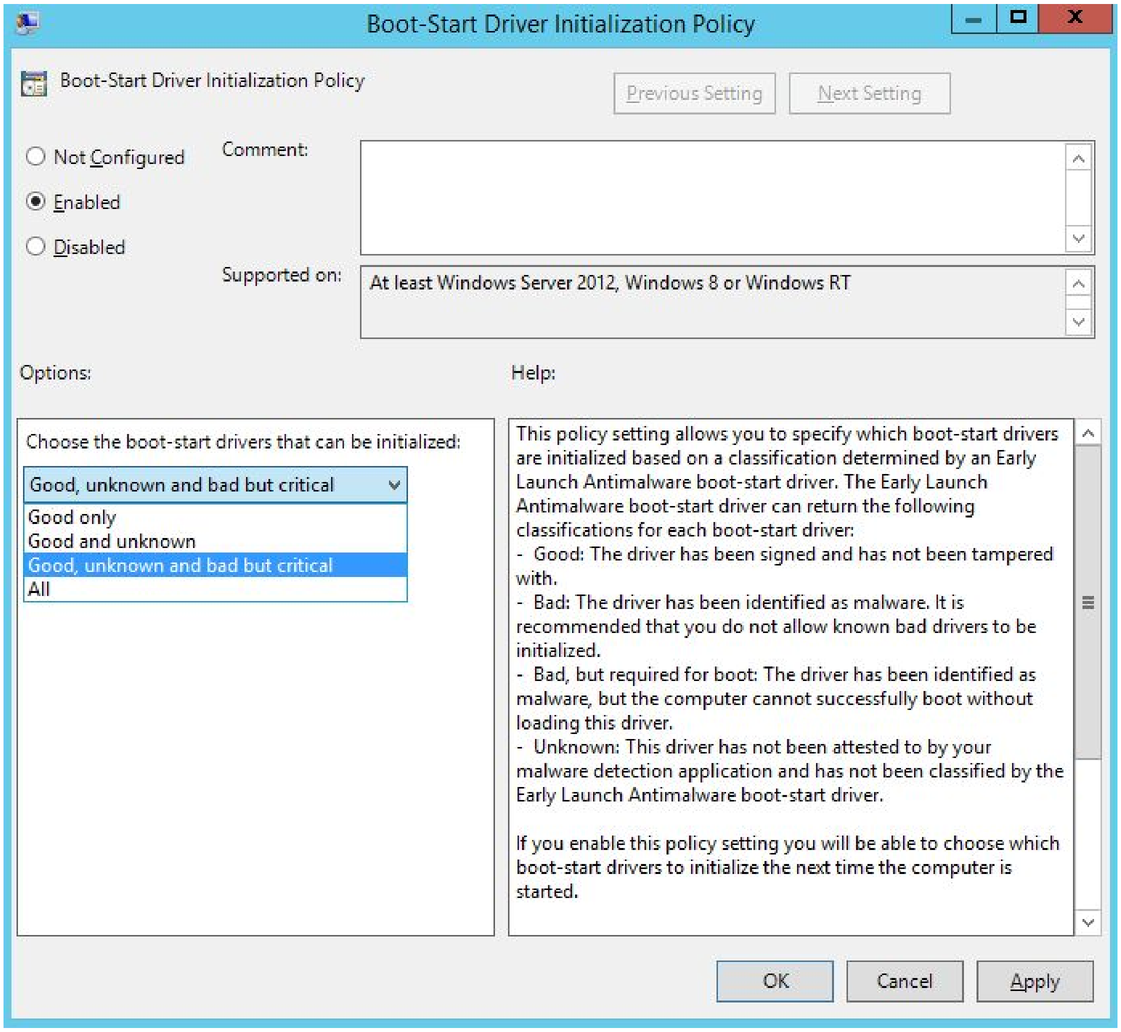
If you enable this policy setting, restricted mode is enforced and participating apps will not delegate credentials to remote computers.

If you disable or do not configure this policy setting, restricted mode is not enforced and participating apps can delegate credentials to remote computers.

Note: To disable most credential delegation, it may be sufficient to deny delegation in Credential Security Support Provider (CredSSP) by modifying Administrative template settings (located at Computer Configuration\Administrative Templates

In Figure 1.2, Windows Server 2012 has enabled the delegation of credentials to remote servers. This means that within restricted mode, it will be enforced and applications will not give credentials to remote computers.

Figure 1.3 – Boot-Start Driver Initialization Policy



Boot-Start Driver Initialization Policy

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Choose the boot-start drivers that can be initialized:

Good, unknown and bad but critical

- Good only
- Good and unknown
- Good, unknown and bad but critical
- All

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:
- Good: The driver has been signed and has not been tampered with.
- Bad: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
- Bad, but required for boot: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
- Unknown: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

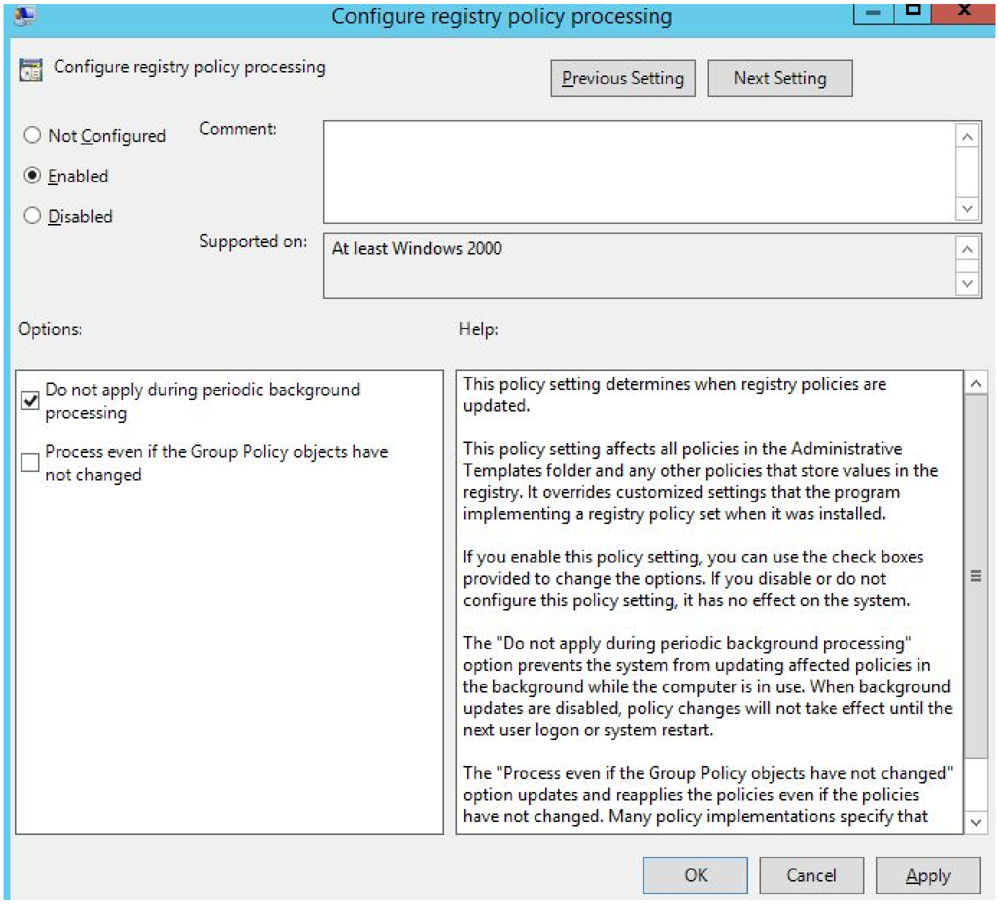
If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started.

This policy allows the user to specify which boot-start drivers are set based on the classification. In Figure 1.3, all of this setting is determined by the "Choose the boot-start drivers that can be initialized". There are three classification that can be selected and they are listed below:

- Good: Driver has been signed and not been tampered with
- Bad: Driver has been identified with malware
- Unknown: Driver has not been attested by malware detection application

Within Windows Server 2012, the recommended selection is "Good, unknown and bad but critical" and that has been selected for this server.

Figure 1.4 – Configure Registry Policy Processing



Configure registry policy processing

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows 2000

☑ Do not apply during periodic background processing

□ Process even if the Group Policy objects have not changed

This policy setting determines when registry policies are updated.

This policy setting affects all policies in the Administrative Templates folder and any other policies that store values in the registry. It overrides customized settings that the program implementing a registry policy set when it was installed.

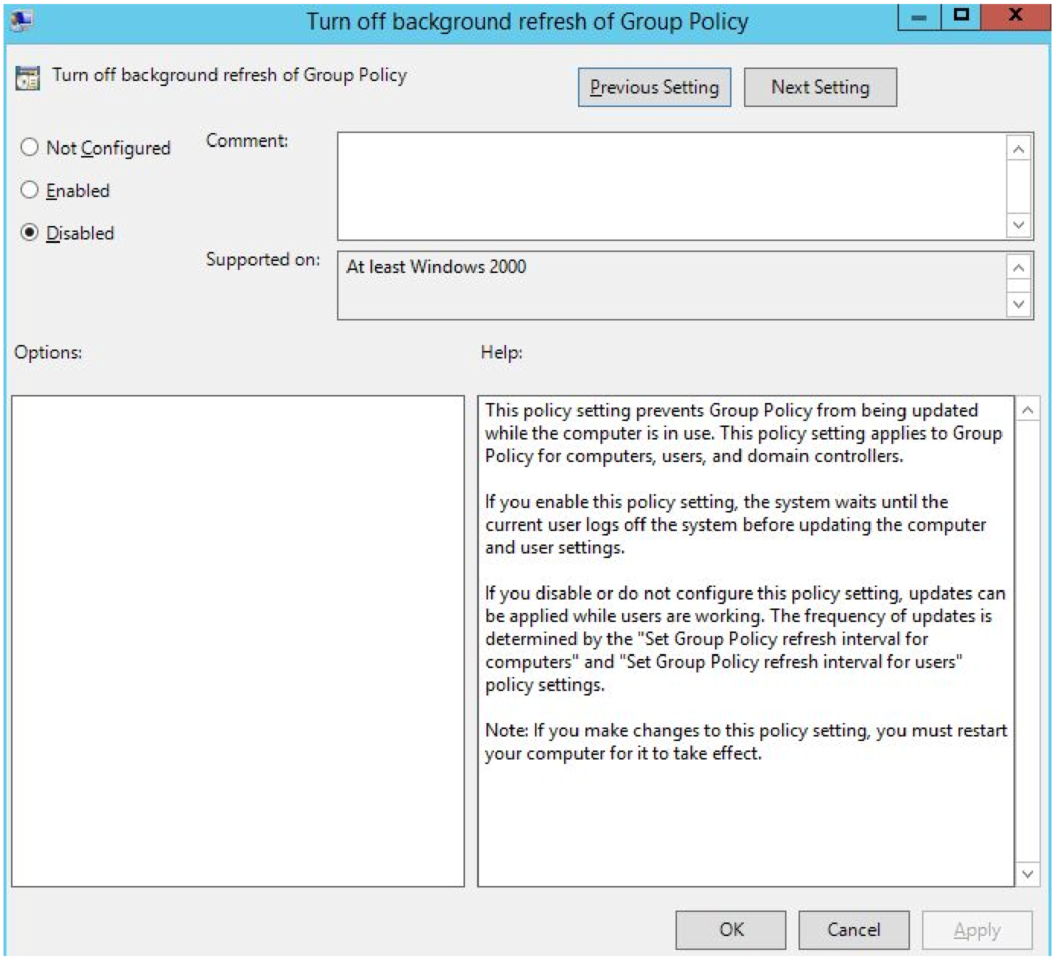
If you enable this policy setting, you can use the check boxes provided to change the options. If you disable or do not configure this policy setting, it has no effect on the system.

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart.

The "Process even if the Group Policy objects have not changed" option updates and reapplies the policies even if the policies have not changed. Many policy implementations specify that

Within this policy, there are 2 possible selections. We have selected the “Do not apply during periodic background processing”. This option stops the system from updating policies while the computer is still running. When the updates are stopped running, the policy will only change until the user restarts their system.

Figure 1.5 – Turn off Background Refresh of Group Policy


Turn off background refresh of Group Policy
Turn off background refresh of Group Policy
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
○ Enabled
● Disabled

Supported on: At least Windows 2000

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users, and domain controllers.

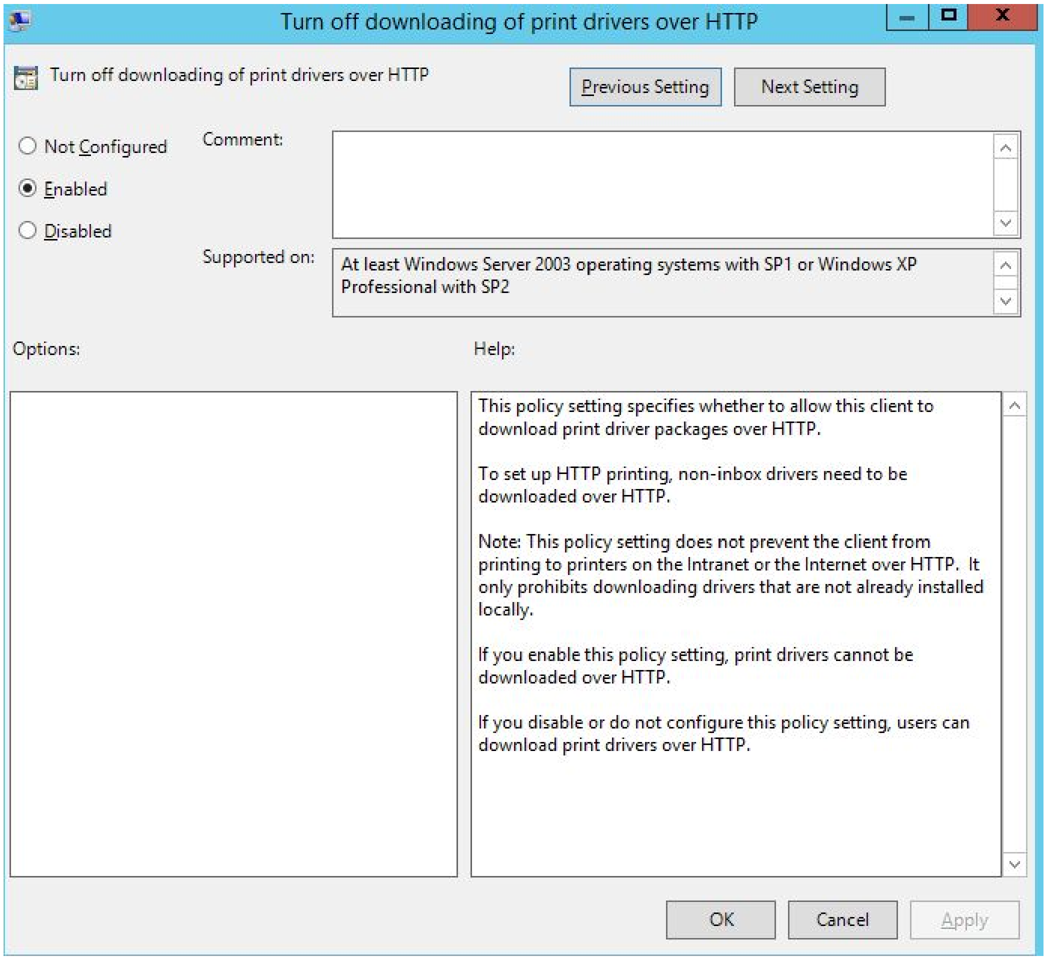
If you enable this policy setting, the system waits until the current user logs off the system before updating the computer and user settings.

If you disable or do not configure this policy setting, updates can be applied while users are working. The frequency of updates is determined by the "Set Group Policy refresh interval for computers" and "Set Group Policy refresh interval for users" policy settings.

Note: If you make changes to this policy setting, you must restart your computer for it to take effect.

This policy prevents the policy from being updated while user is still using the computer. It is mainly applied to computers, users and domain controllers. However, with this policy being disabled, updates can still applied while users are working.

Figure 1.6 – Turn off Downloading of print drivers over HTTP



Turn off downloading of print drivers over HTTP
Turn off downloading of print drivers over HTTP
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows Server 2003 operating systems with SP1 or Windows XP Professional with SP2

This policy setting specifies whether to allow this client to download print driver packages over HTTP.

To set up HTTP printing, non-inbox drivers need to be downloaded over HTTP.

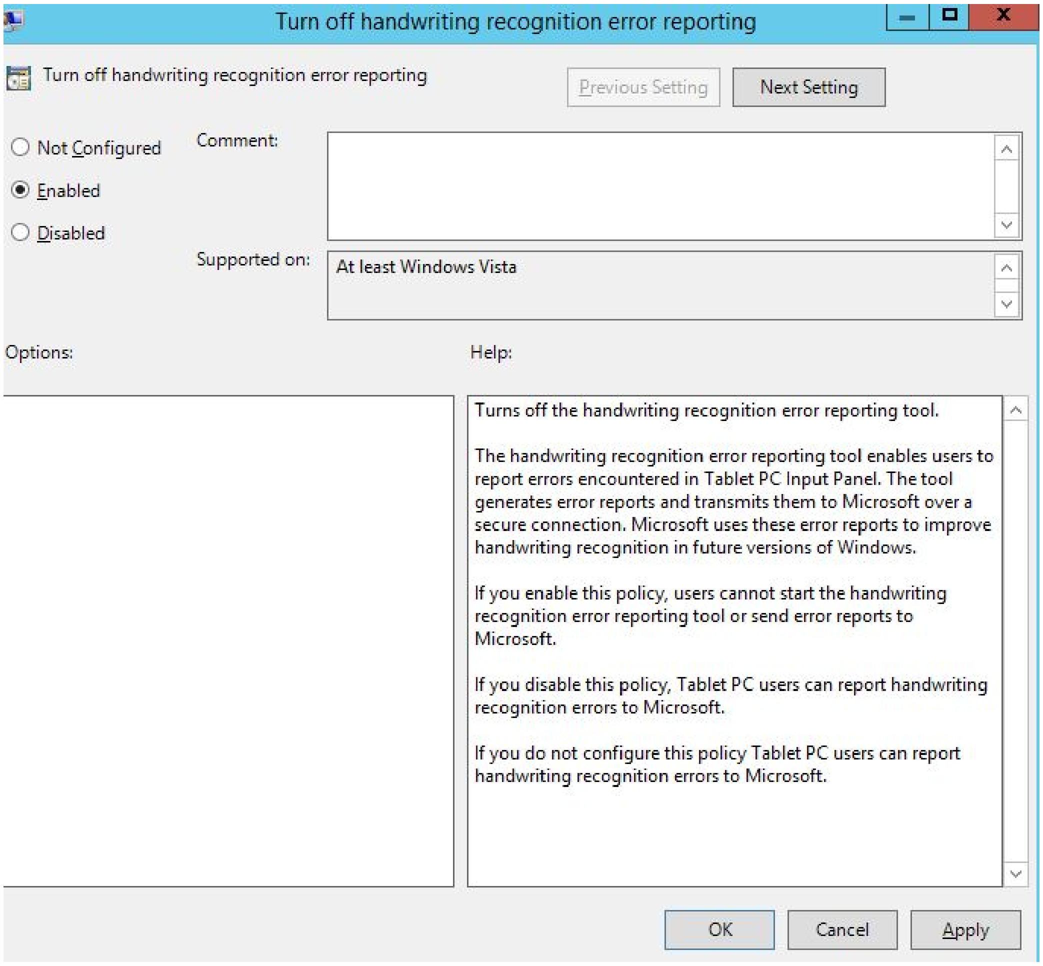
Note: This policy setting does not prevent the client from printing to printers on the Intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

If you enable this policy setting, print drivers cannot be downloaded over HTTP.

If you disable or do not configure this policy setting, users can download print drivers over HTTP.

In Figure 1.6, this policy demonstrates the ability whether the computer can download print driver packages or not. In order to setup this driver, the download must be done over HTTP.

Figure 1.7 – Turn off Handwriting Recognition Error Reporting



Turn off handwriting recognition error reporting
Turn off handwriting recognition error reporting
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

Turns off the handwriting recognition error reporting tool.

The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows.

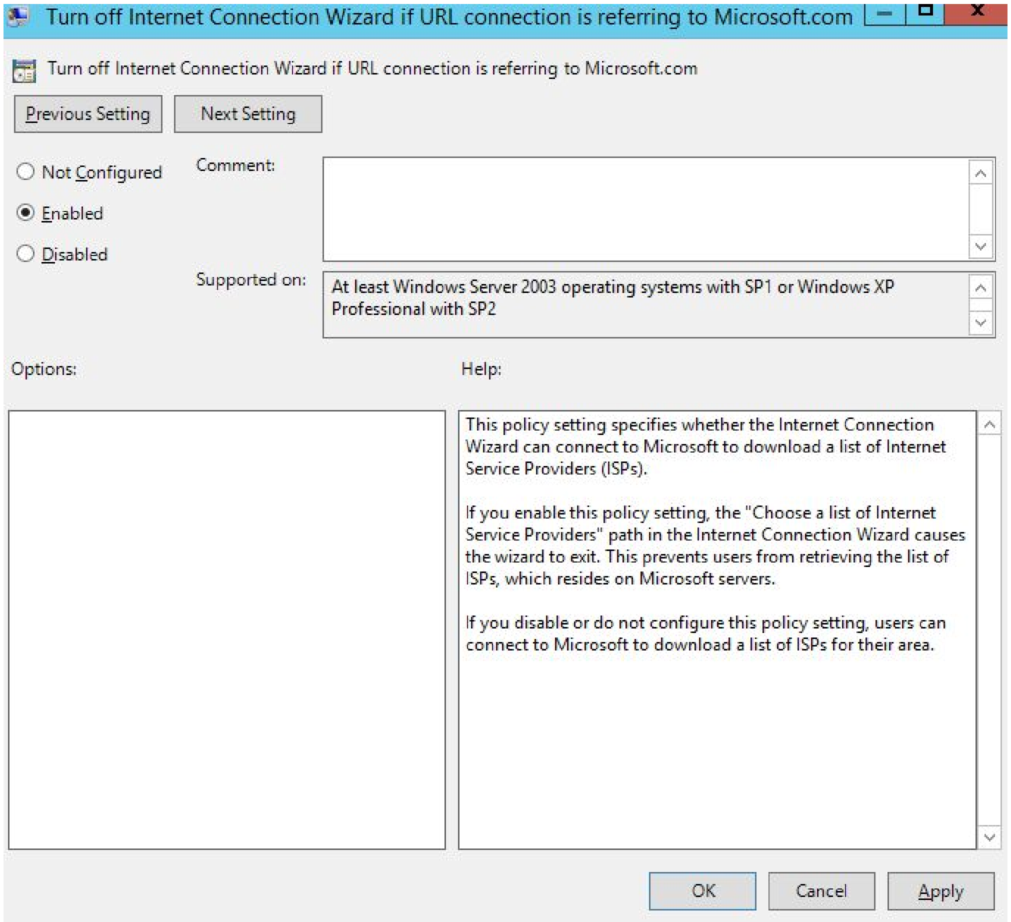
If you enable this policy, users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

If you disable this policy, Tablet PC users can report handwriting errors to Microsoft.

If you do not configure this policy Tablet PC users can report handwriting recognition errors to Microsoft.

Figure 1.7 shows that the handwriting recognition error reporting has been enabled. This allows users to report any problems within the Tablet PC input Panel. With this tool, it creates error report and sends them to Microsoft. Microsoft will then use the error report to improve it in their future Windows. It is not acceptable to upload a person's handwriting without approval by its user.

Figure 1.8 – Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com



Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com

Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems with SP1 or Windows XP Professional with SP2

Options:

Help:

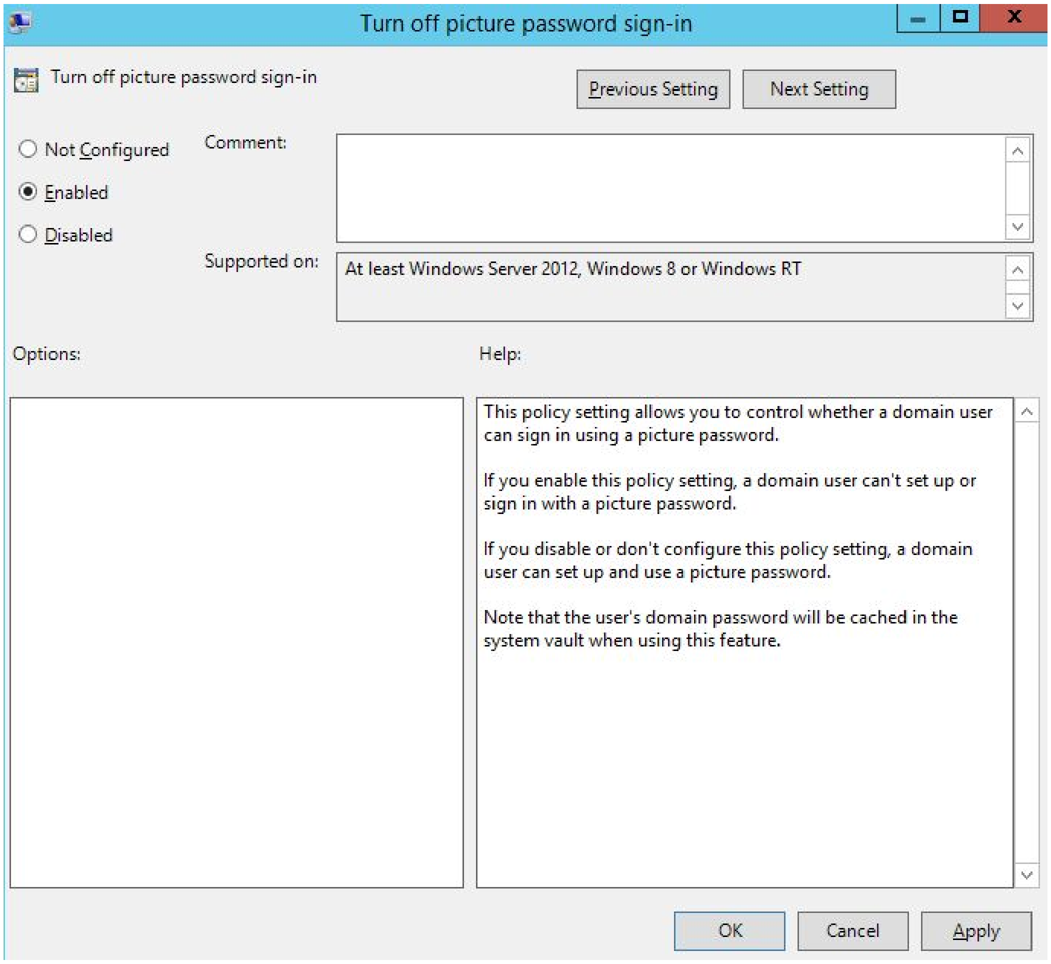
This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs).

If you enable this policy setting, the "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

If you disable or do not configure this policy setting, users can connect to Microsoft to download a list of ISPs for their area.

In Figure 1.8, it has this policy enabled. This policy specifies whether the internet connection wizard can connect to the Microsoft's page and download the list of ISP.

Figure 1.9 – Turn off Picture Password Sign-in



○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

This policy setting allows you to control whether a domain user can sign in using a picture password.

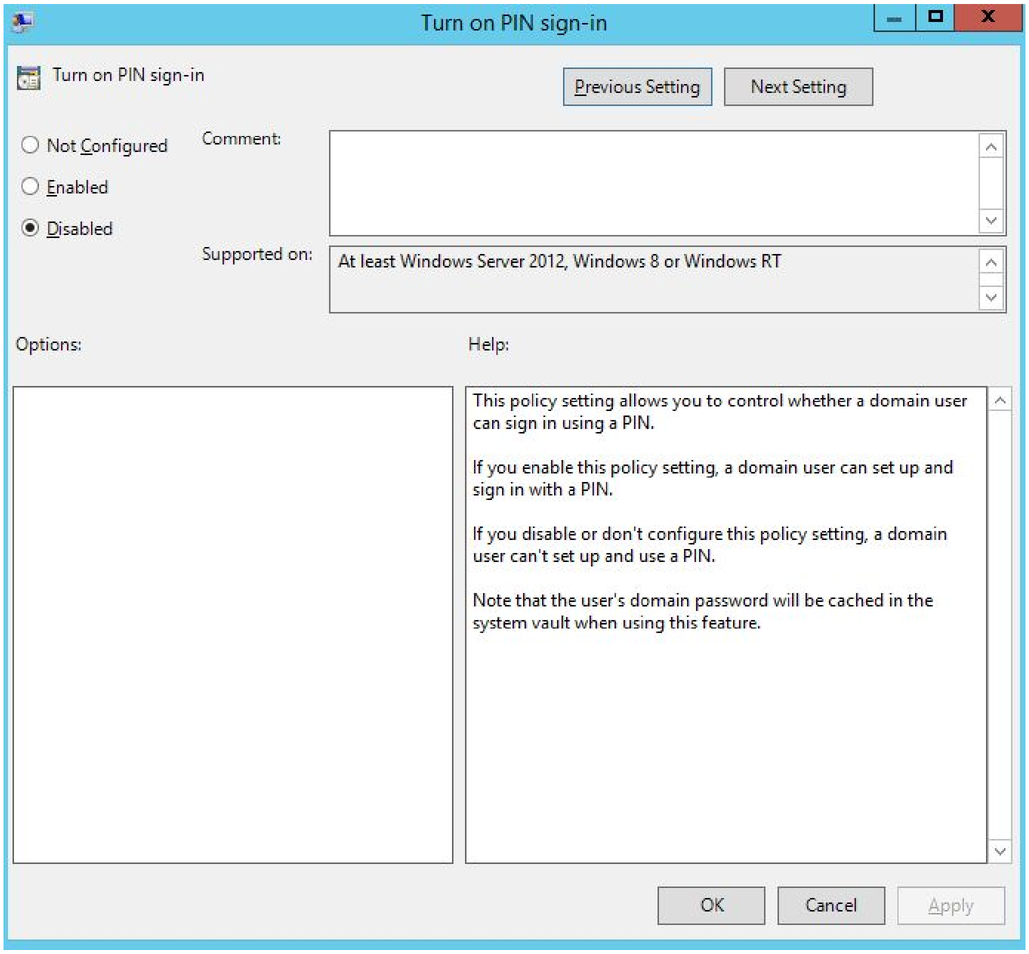
If you enable this policy setting, a domain user can't set up or sign in with a picture password.

If you disable or don't configure this policy setting, a domain user can set up and use a picture password.

Note that the user's domain password will be cached in the system vault when using this feature.

As shown in Figure 1.9, this setting allows users to control whether a user can sign in using a picture password. With a picture password, there is no requirement for a typed password. Users should be extra cautious when working in a big environment because with a glimpse of the users' picture password, the potential hacker can surf the web for a similar picture that allows that hacker to access the users system.

Figure 1.10 – Turn on PIN Sign-In



○ Not Configured
○ Enabled
● Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

This policy setting allows you to control whether a domain user can sign in using a PIN.

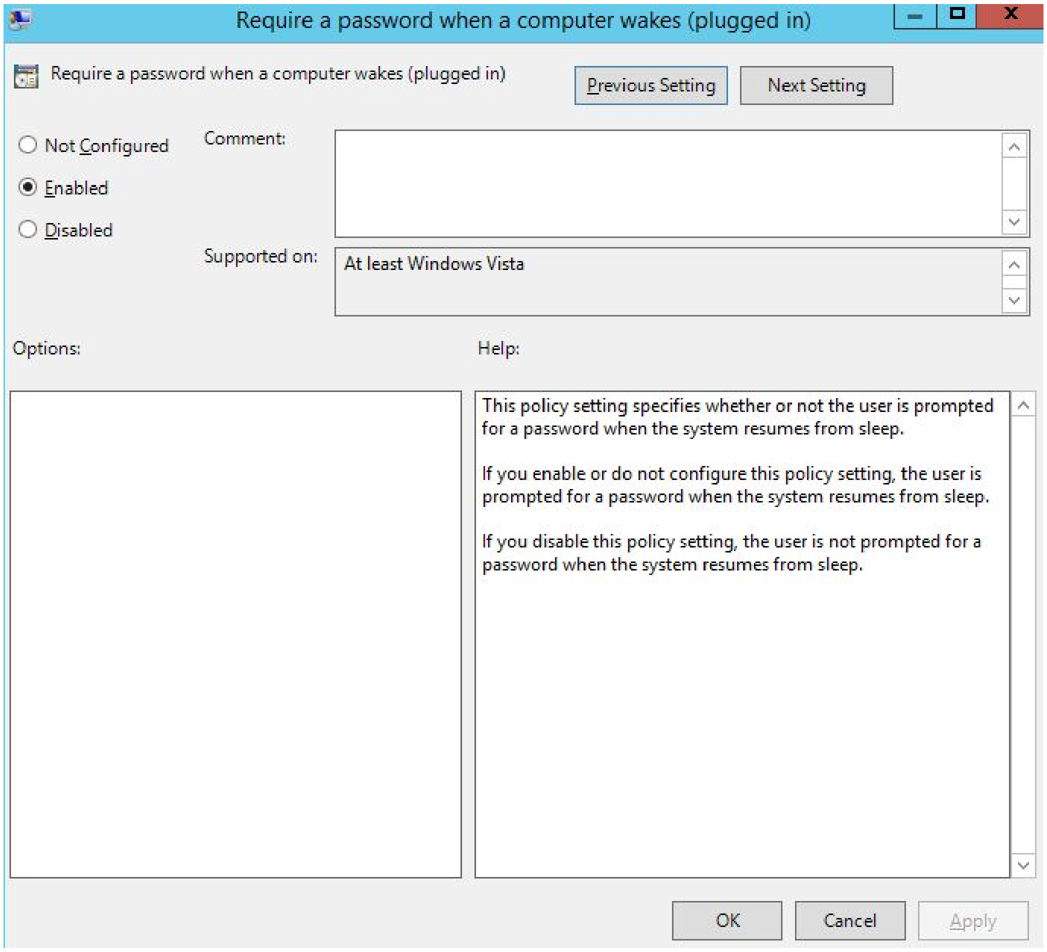
If you enable this policy setting, a domain user can set up and sign in with a PIN.

If you disable or don't configure this policy setting, a domain user can't set up and use a PIN.

Note that the user's domain password will be cached in the system vault when using this feature.

In Figure 1.10, this policy determines whether a user can sign in using a PIN only. With this policy disabled, this means that users cannot create or sign in using a PIN.

Figure 1.11 – Require a Password When a Computer Wakes



Require a password when a computer wakes (plugged in)

Require a password when a computer wakes (plugged in)

○ Not Configured

● Enabled

○ Disabled

Supported on: At least Windows Vista

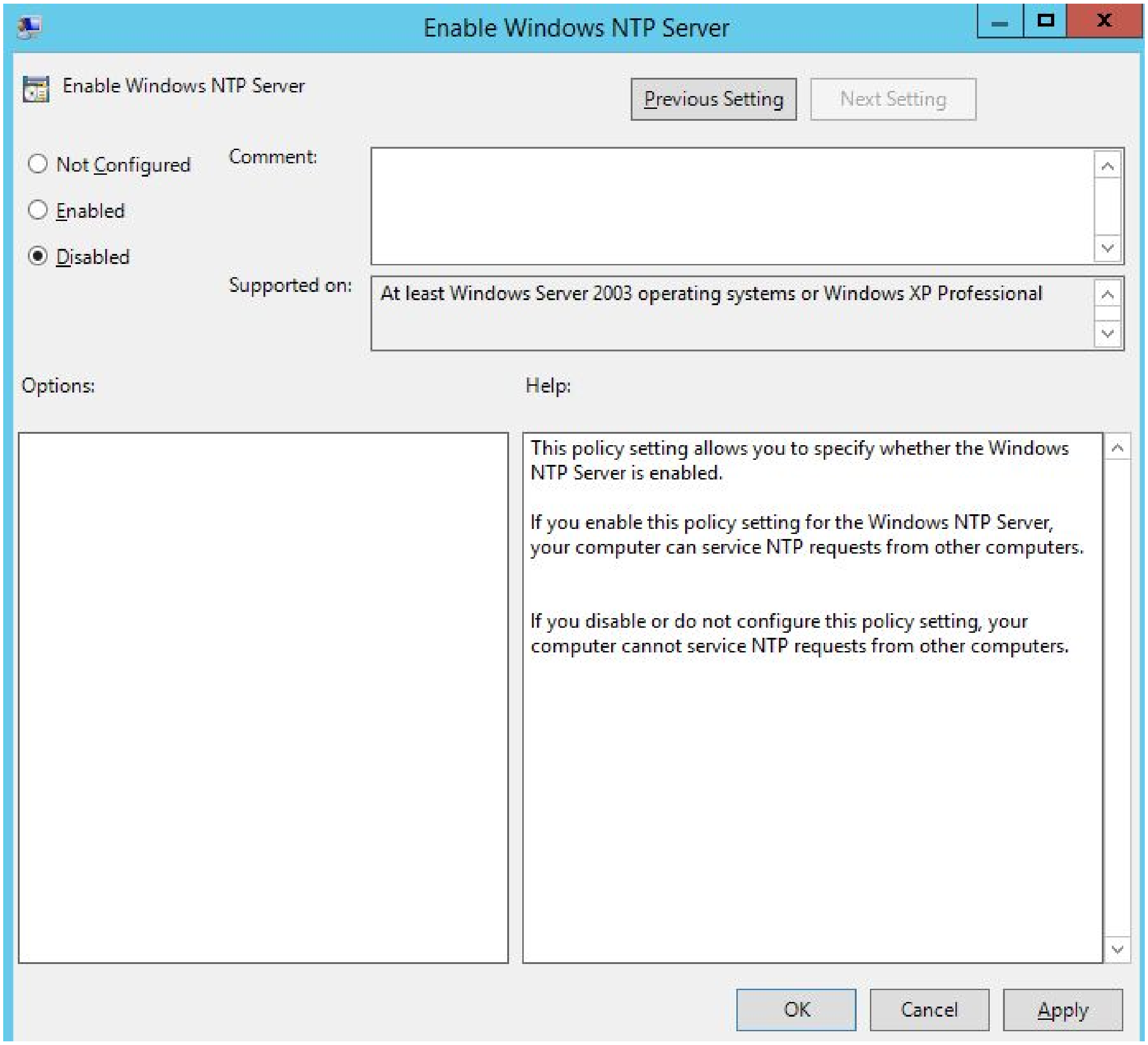
This policy setting specifies whether or not the user is prompted for a password when the system resumes from sleep.

If you enable or do not configure this policy setting, the user is prompted for a password when the system resumes from sleep.

If you disable this policy setting, the user is not prompted for a password when the system resumes from sleep.

In Figure 1.11, the policy specifics whether a user will be prompt for user login from sleep. When user logs in from sleep, they will be required to provide logon credentials in order to access the system.

Figure 1.12 – Enable Windows NTP Server



Enable Windows NTP Server

Enable Windows NTP Server

○ Not Configured

○ Enabled

● Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

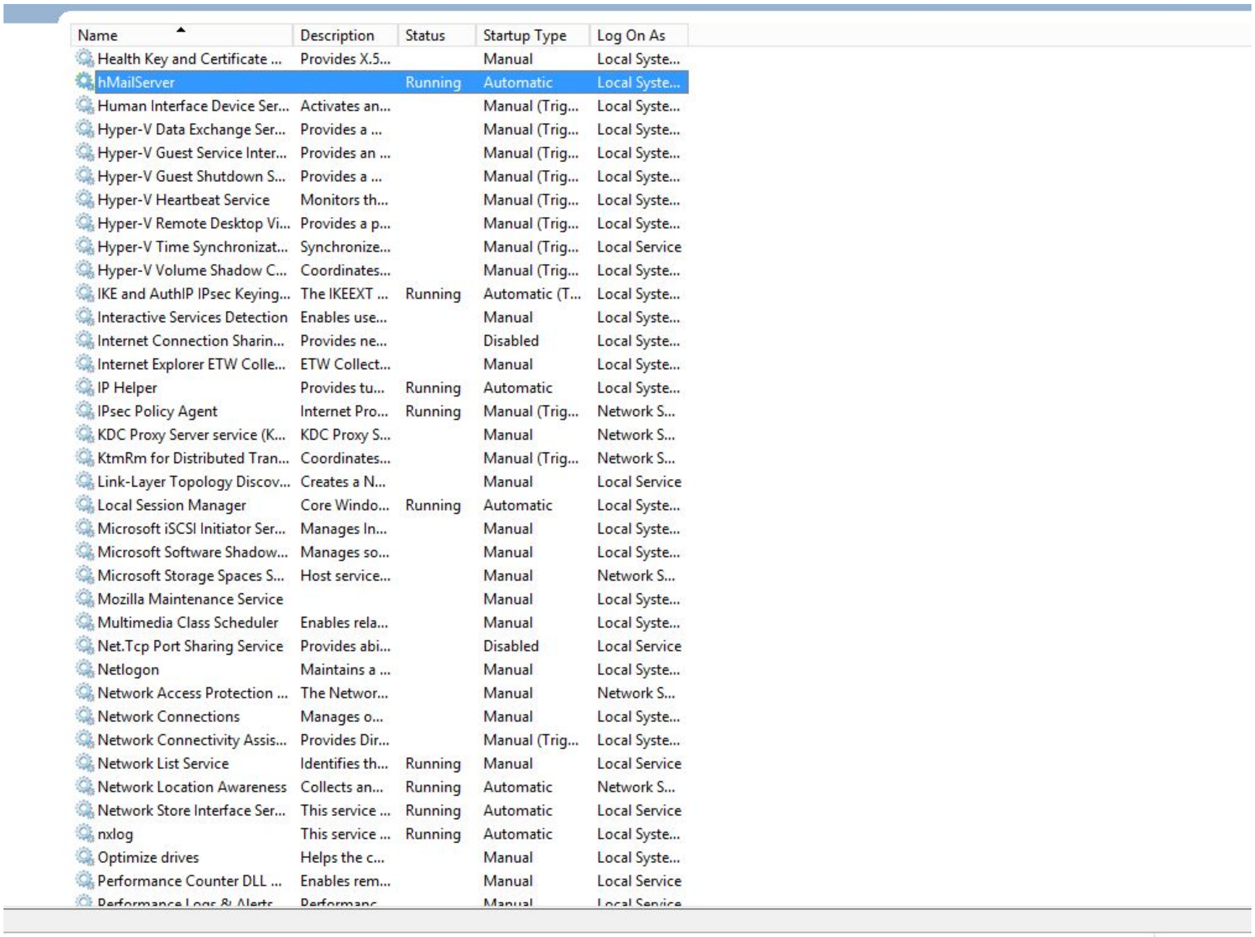
This policy setting allows you to specify whether the Windows NTP Server is enabled.

If you enable this policy setting for the Windows NTP Server, your computer can service NTP requests from other computers.

If you disable or do not configure this policy setting, your computer cannot service NTP requests from other computers.

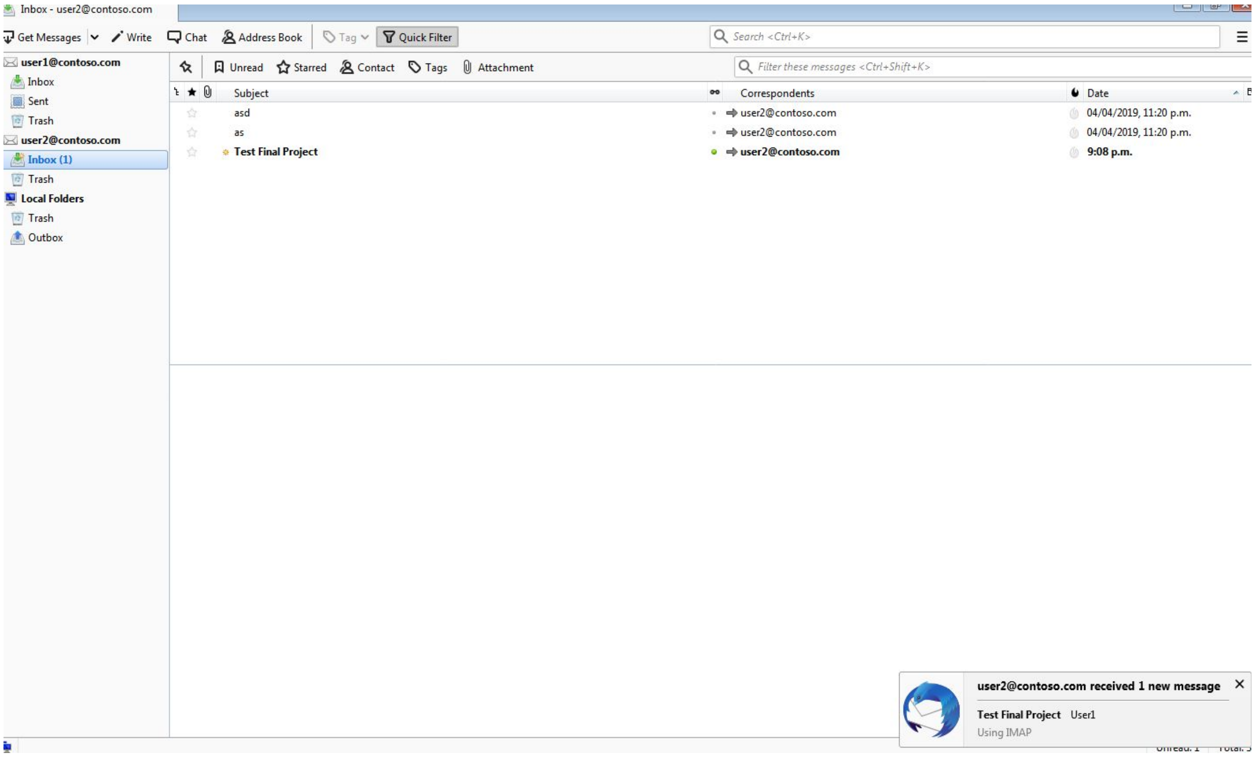
In Figure 1.12, we have the “Enable Windows NTP Server” disabled. What this does is that, it makes the computer unable to service NTP requests from other computers. NTP is a protocol for clock synchronization between computers in a network.

Figure 1.13 - HmailServer



Name	Description	Status	Startup Type	Log On As
Health Key and Certificate ...	Provides X.5...		Manual	Local Syste...
hMailServer		Running	Automatic	Local Syste...
Human Interface Device Ser...	Activates an...		Manual (Trig...	Local Syste...
Hyper-V Data Exchange Ser...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Guest Service Inter...	Provides an ...		Manual (Trig...	Local Syste...
Hyper-V Guest Shutdown S...	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Heartbeat Service	Monitors th...		Manual (Trig...	Local Syste...
Hyper-V Remote Desktop Vi...	Provides a p...		Manual (Trig...	Local Syste...
Hyper-V Time Synchronizat...	Synchronize...		Manual (Trig...	Local Service
Hyper-V Volume Shadow C...	Coordinates...		Manual (Trig...	Local Syste...
IKE and AuthIP IPsec Keying...	The IKEEXT ...	Running	Automatic (T...	Local Syste...
Interactive Services Detection	Enables use...		Manual	Local Syste...
Internet Connection Sharin...	Provides ne...		Disabled	Local Syste...
Internet Explorer ETW Colle...	ETW Collect...		Manual	Local Syste...
IP Helper	Provides tu...	Running	Automatic	Local Syste...
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Network S...
KDC Proxy Server service (K...	KDC Proxy S...		Manual	Network S...
KtmRm for Distributed Tran...	Coordinates...		Manual (Trig...	Network S...
Link-Layer Topology Discov...	Creates a N...		Manual	Local Service
Local Session Manager	Core Windo...	Running	Automatic	Local Syste...
Microsoft iSCSI Initiator Ser...	Manages In...		Manual	Local Syste...
Microsoft Software Shadow...	Manages so...		Manual	Local Syste...
Microsoft Storage Spaces S...	Host service...		Manual	Network S...
Mozilla Maintenance Service			Manual	Local Syste...
Multimedia Class Scheduler	Enables rela...		Manual	Local Syste...
Net.Tcp Port Sharing Service	Provides abi...		Disabled	Local Service
Netlogon	Maintains a ...		Manual	Local Syste...
Network Access Protection ...	The Networ...		Manual	Network S...
Network Connections	Manages o...		Manual	Local Syste...
Network Connectivity Assis...	Provides Dir...		Manual (Trig...	Local Syste...
Network List Service	Identifies th...	Running	Manual	Local Service
Network Location Awareness	Collects an...	Running	Automatic	Network S...
Network Store Interface Ser...	This service ...	Running	Automatic	Local Service
nxlog	This service ...	Running	Automatic	Local Syste...
Optimize drives	Helps the c...		Manual	Local Syste...
Performance Counter DLL ...	Enables rem...		Manual	Local Service
Performance Logs & Alerts	Performanc...		Manual	Local Service

Figure 1.14 – HmailServer



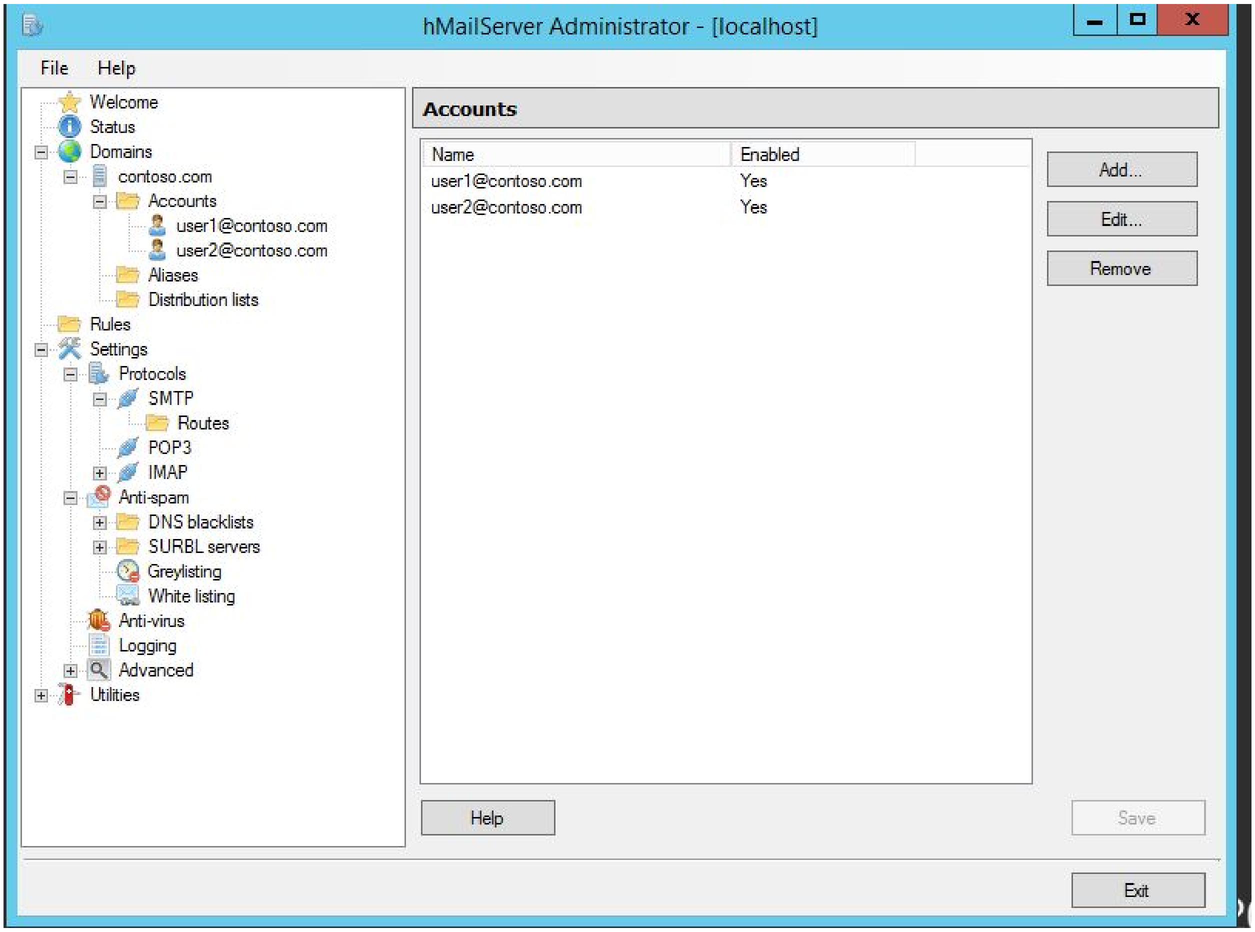
Subject	Correspondents	Date
asd	user2@contoso.com	04/04/2019, 11:20 p.m.
as	user2@contoso.com	04/04/2019, 11:20 p.m.
Test Final Project	**user2@contoso.com**	**9:08 p.m.**

user2@contoso.com received 1 new message

Test Final Project User1

Using IMAP

Figure 1.15 – HmailServer

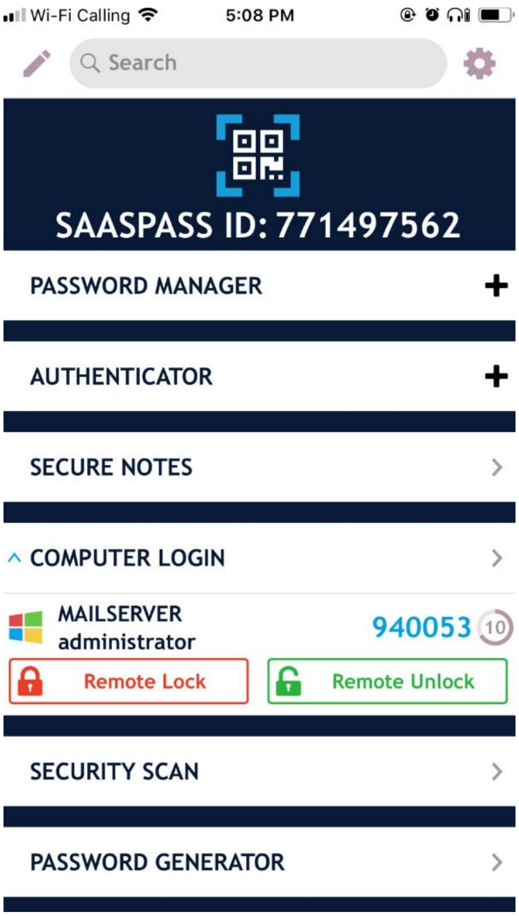


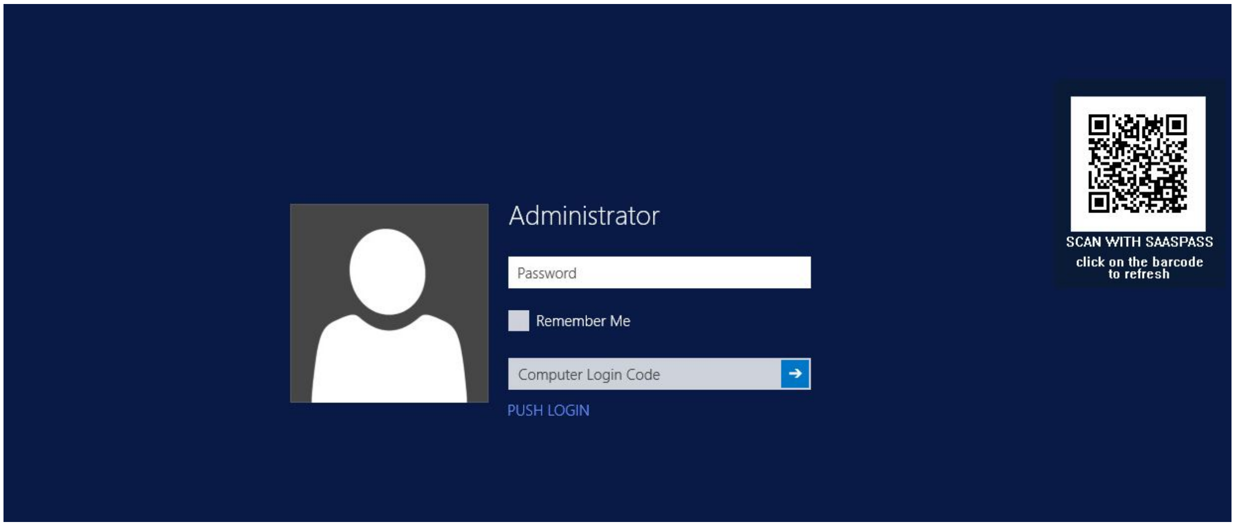
Name	Enabled
user1@contoso.com	Yes
user2@contoso.com	Yes

In Figures 1.13, 1.14 and 1.15 hMailServer is configured and running. It is a free, email server for Microsoft Windows. It supports all forms of protocols and to list a few; IMAP, SMTP and POP3. In Figure 1.15, it illustrates what we as a group have installed on hMailServer and they include:

- Open Source
- Built-In Anti –Spam
  - Spam protection
  - Scan both incoming and outgoing emails
- Anti-virus installed
- Greylisting
  - Method of defending email against email (mainly spam)
- DNS Blacklist
  - Spam blocking lists that blocks messages from system

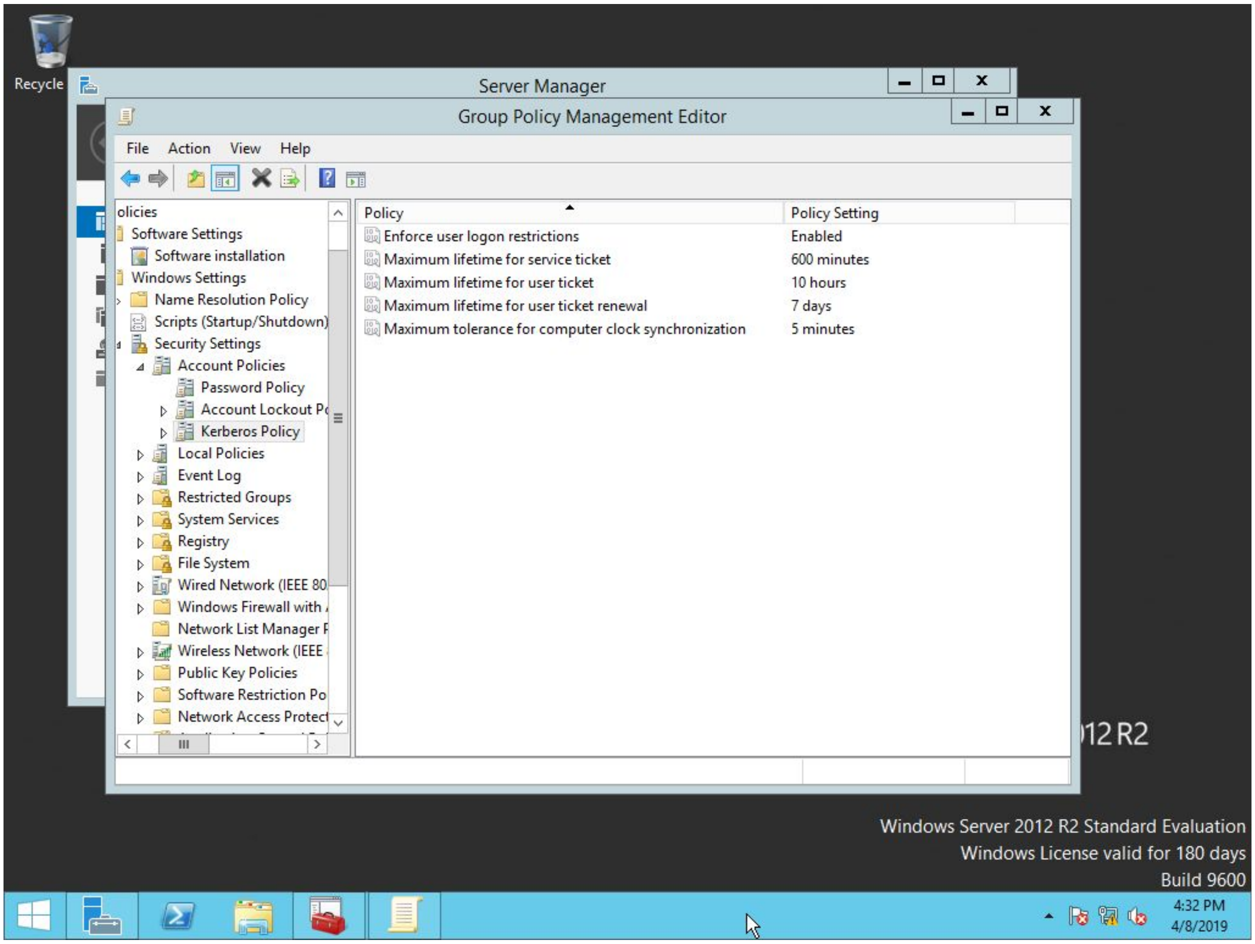
Figure 1.16 - SAASPASS





In Windows Sever 2012, we have installed SAASPASS as a security measure to prevent unauthorized users from attempting to log in. It is a two-factor authentication and secure single sign on for the computer. This tool prevents and reduces the risk of hackers by allowing users to sign-in and authenticate with a single click and through a one-time password. Log in can be done through Barcode scan, proximity and on device log in.

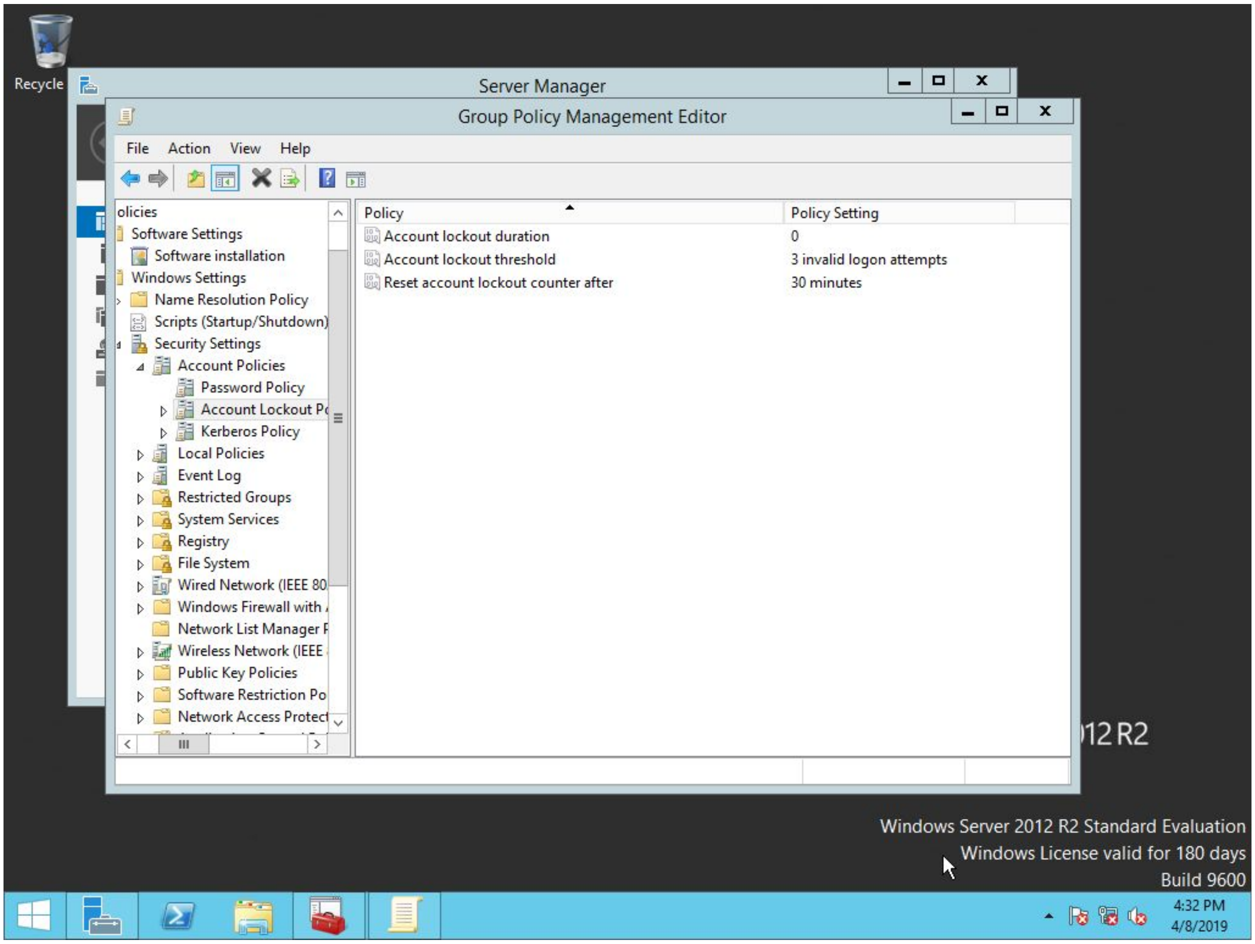
Figure 1.17 – Group Policy Management Editor



Policy	Policy Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

In Figure 1.17, we have “enforce user logon restrictions” enabled. What this does is that, it decides whether KDC confirms every request for a ticket against the user account. Also, with the “maximum lifetime for service ticket” up to 600 minutes, this indicates that a user can have access to a particular service for over 600 minutes. Last but not least, the “maximum lifetime for user ticket renewal” of 7 days means that the user can renew their ticket every 7 days.

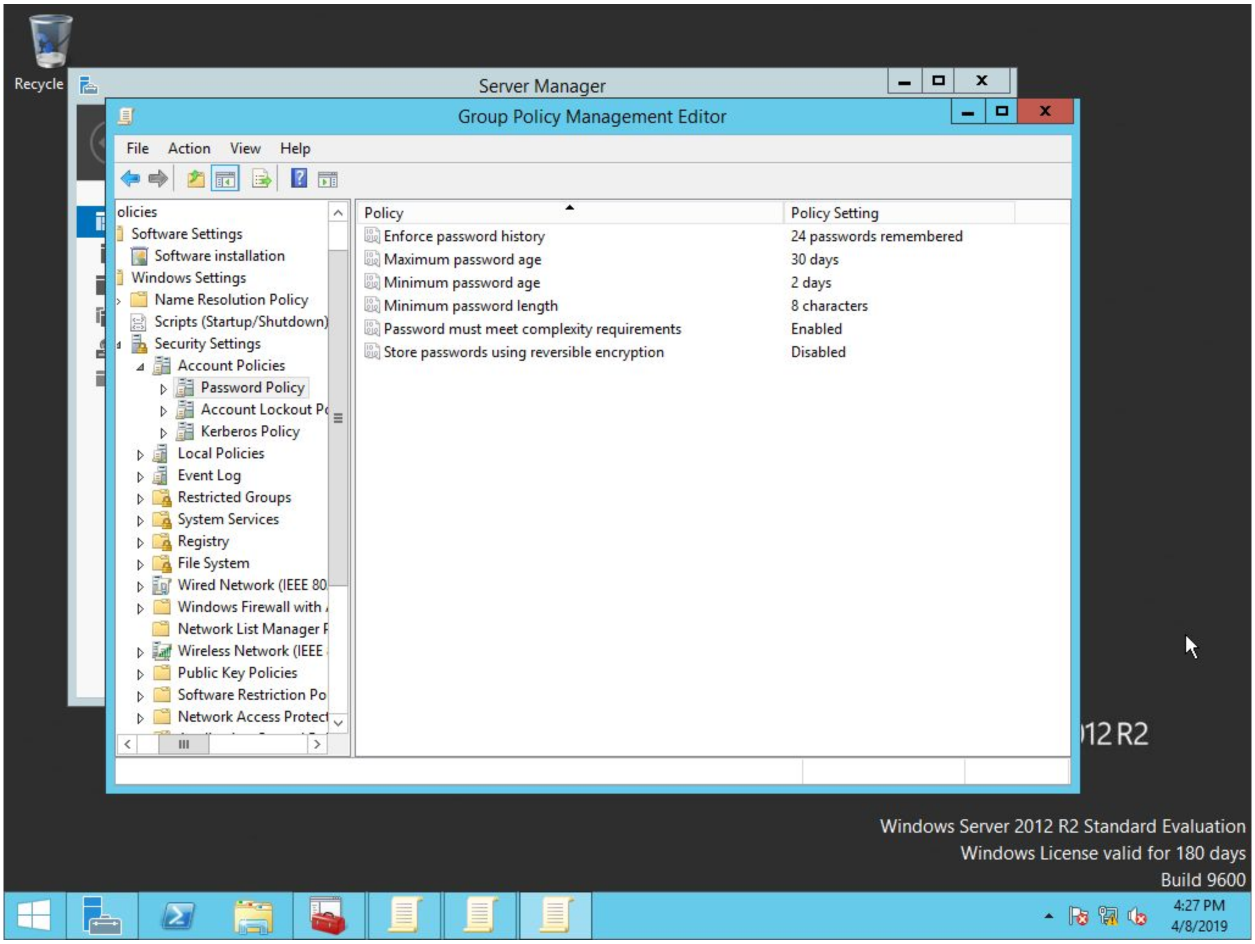
Figure 1.18 – Group Policy Management Editor



Policy	Policy Setting
Account lockout duration	0
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

As shown in Figure 1.18, we have “Account Lockout Duration” set to 0. 0 indicates that after a specific number of log in attempts, user accounts will remain locked until an administrator unlocks it. Next we have “Account lockout threshold set to 3”. This means that the user has 3 log in attempts and if unable to log in, the user will be locked out. In cases if it was set to “0”, user has unlimited log in attempts.

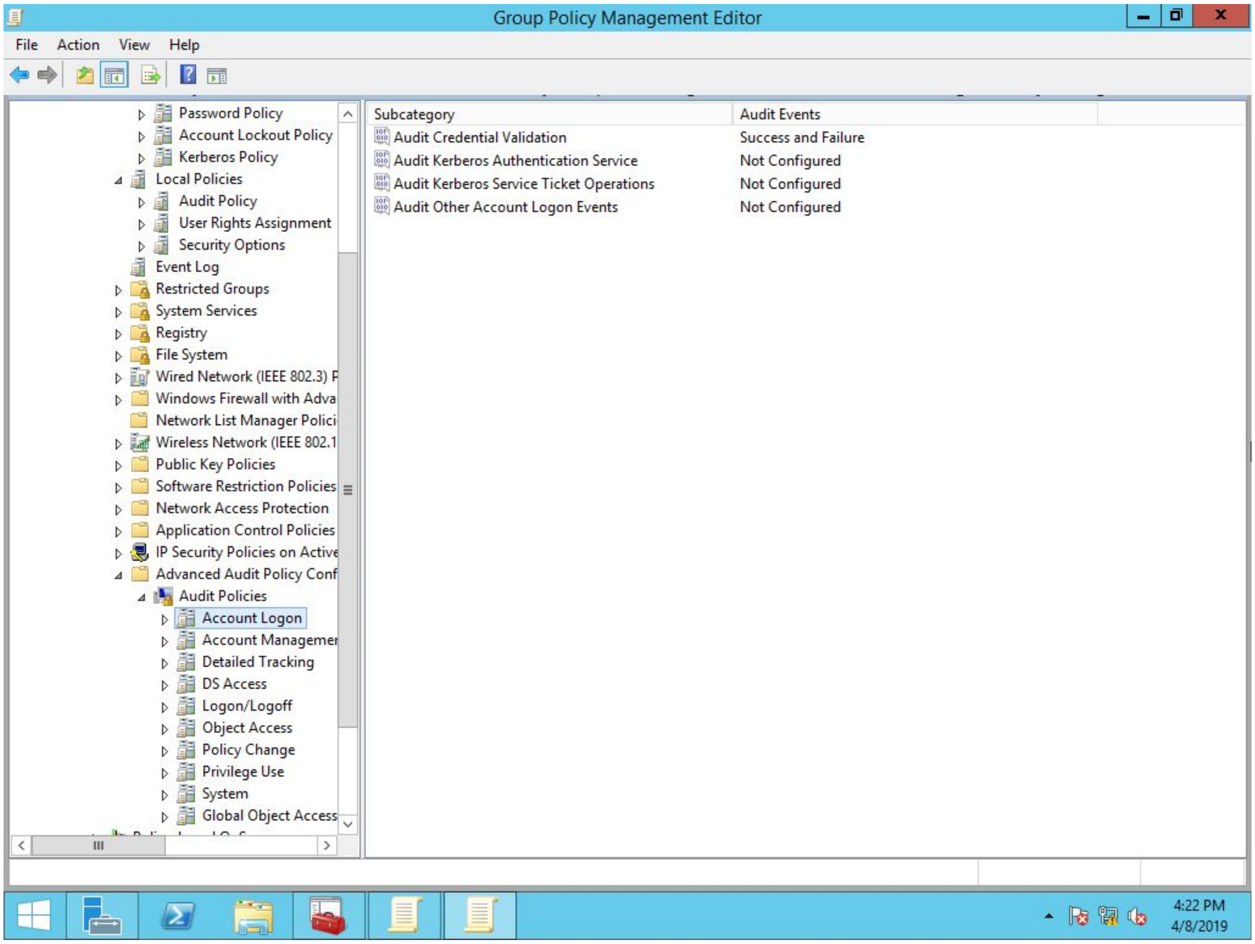
Figure 1.19 – Group Policy Management Editor



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	30 days
Minimum password age	2 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

In Figure 1.19, we have set the enforce password history and maximum password age as 24 passwords remembered and 30 days. This helps reduce liabilities that causes users to reuse the same passwords over and over again and after 30 days, a password reset will be performed. We have also set the least number of characters for a password to 8 characters. This will be long enough for security reasons and enough for users to consistently remember the passwords.

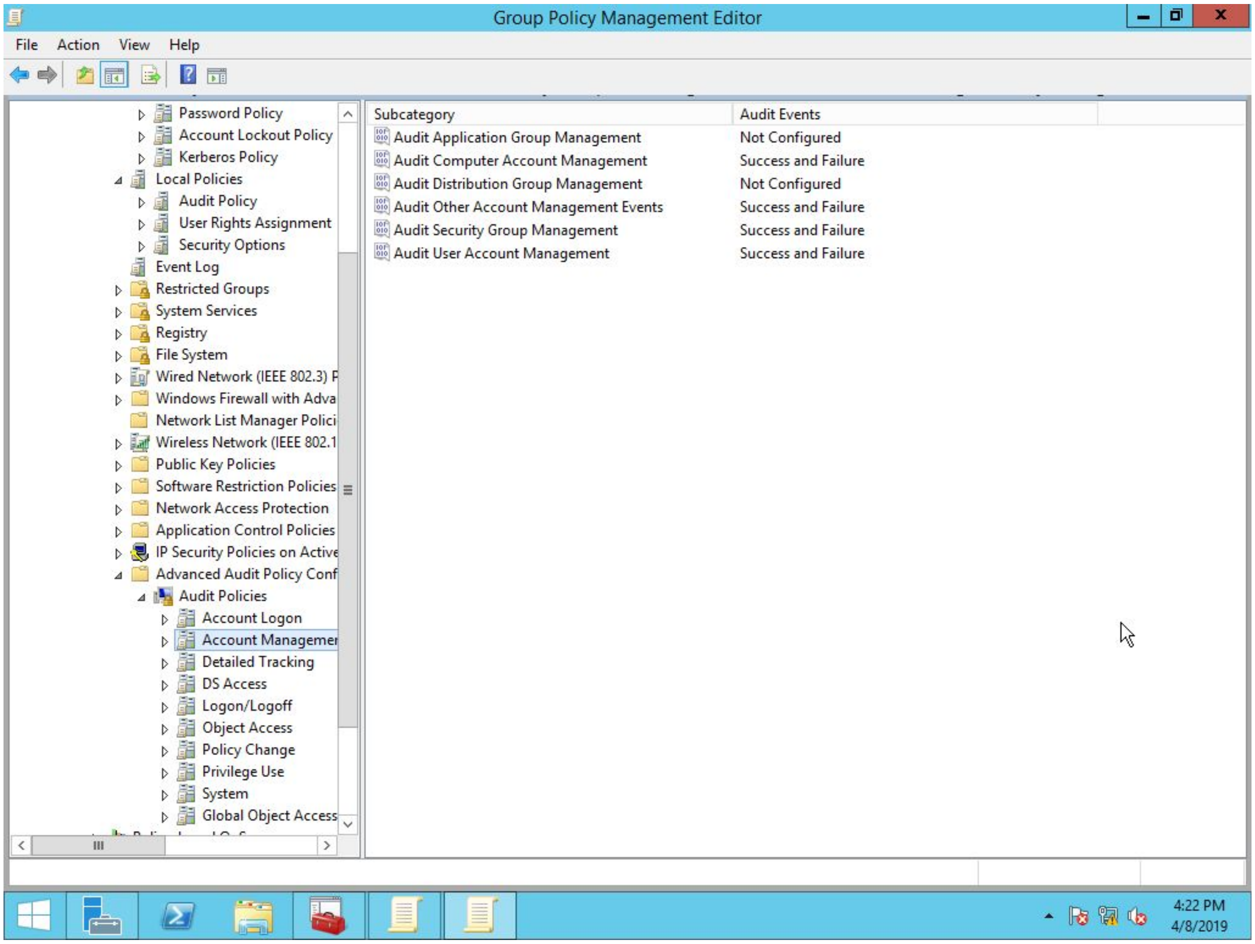
Figure 1.20 – Group Policy Management Editor



Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

In Figure 1.20, with the "Audit Credential Validation" configured to "success and failure", this is great for handling and monitoring unsuccessful attempts from outsiders to attempt "brute-force" attacks, account compromise on domain controller and retrieving account information.

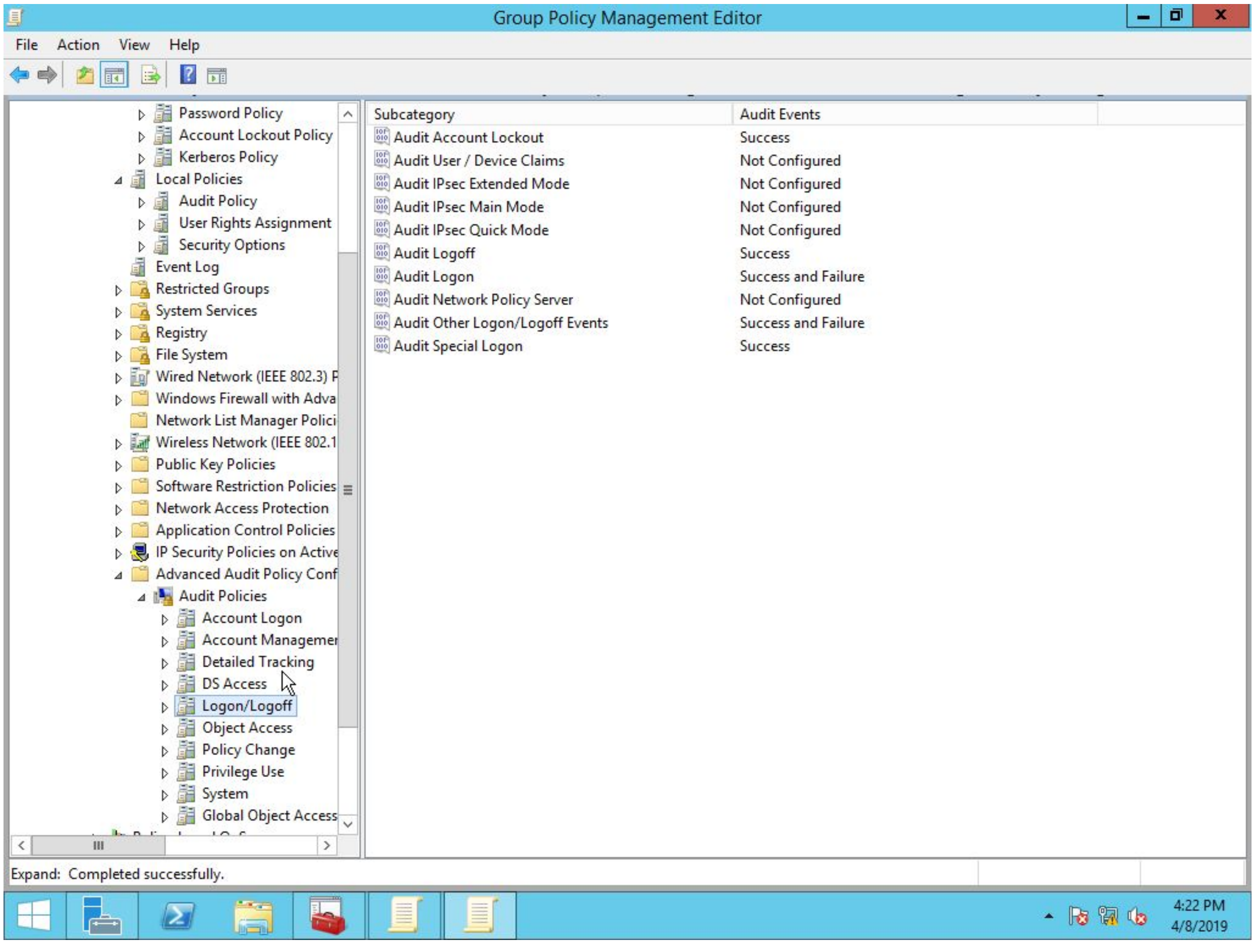
Figure 1.21 – Group Policy Management Editor



Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

In Figure 1.21, we have configured “Audit computer account management”, “Audit other Account management events”, “Audit security group management” and “Audit user account management”. This allows system administrator to keep track of any changes that happen to a user that on a domain. As well, we can audit events based on changes done in security groups, members and group changes on a basis.

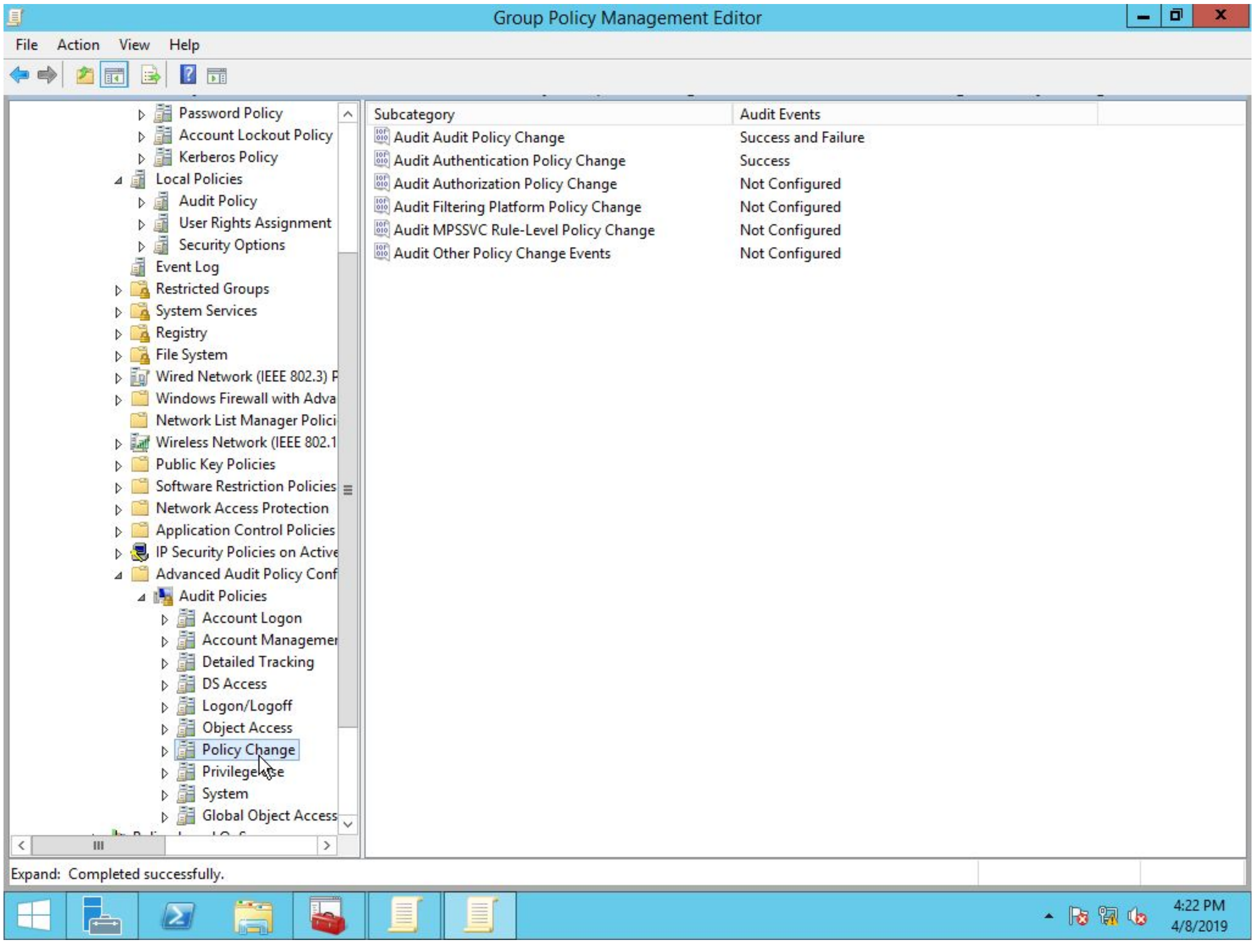
Figure 1.22 – Group Policy Management Editor



Subcategory	Audit Events
Audit Account Lockout	Success
Audit User / Device Claims	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success

In Figure 1.22, an audit event will be created when a user is unable to log onto the computer because they locked themselves out (due to a number of login attempts). This is great because it helps understand what users do on their accounts and detects any potential attacks. To add on, it also generates audit events when a user attempts a log in. Examples of things that are recorded are; logon success and failure rates, SID being filtered and logging in with explicit identifications.

Figure 1.23 – Group Policy Management Editor



Subcategory	Audit Events
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Not Configured
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Not Configured
Audit Other Policy Change Events	Not Configured

Expand: Completed successfully.

Under Figure 1.23, it determines whether the OS creates an audit event when there are changes made to the authentication policy. A few of the things that change the policy are listed below:

- Changes made in forest
- Logon as service
- Logon as batch jobs
- Logon locally

References

- Dansimp. “Threat Protection (Windows 10).” *(Windows 10) | Microsoft Docs*, docs.microsoft.com/en-us/windows/security/threat-protection/.

- *CIS Microsoft Windows Server 2012 R2 Benchmark*. www.cisecurity.org/wp-content/uploads/2017/04/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0.pdf.