IT Security

Windows Server Hardening Guide
(English Version)

August 2022

Education Bureau

Table of Contents

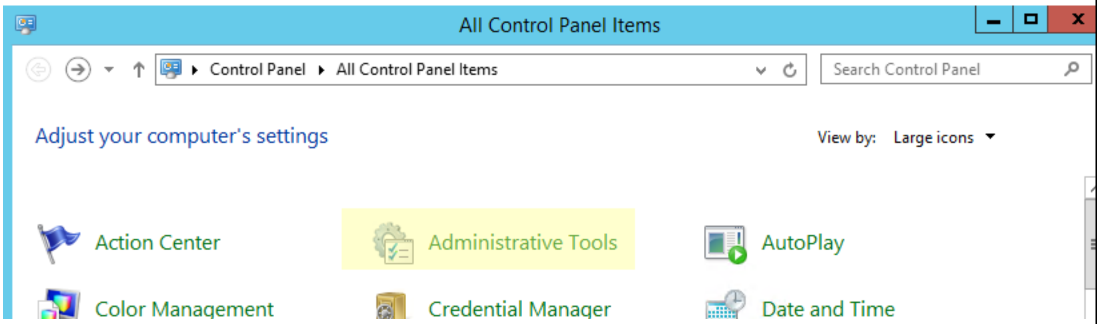
1. Windows Installation

- ✓ Disable any unneeded services included in the default installation
- ✓ Remove unnecessary Windows Server roles and features
- ✓ Consider to use EFS with NTFS file system or BitLocker encryption for restricted data
- ✓ Assign a static IP for server
- ✓ Run Windows update to install all security updates or patches
- ✓ Run Antivirus update to install the latest antivirus definition
- ✓ Enable automatic notification of patch availability and make sure that all appropriate patches, hotfixes and service packs are reviewed, tested and applied in a timely manner
- ✓ It is not recommended to install client-side software, such as Chrome, Adobe Flash, pdf viewers etc. on server

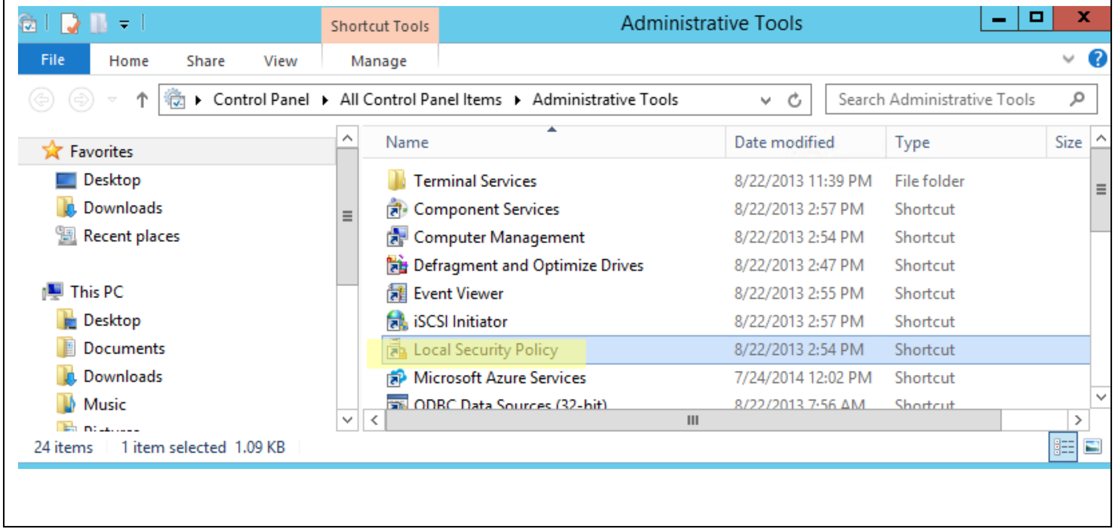
2. Security Configuration

2.1 Network Security and Access Management

In All Control Panel Items , click Administrative Tools



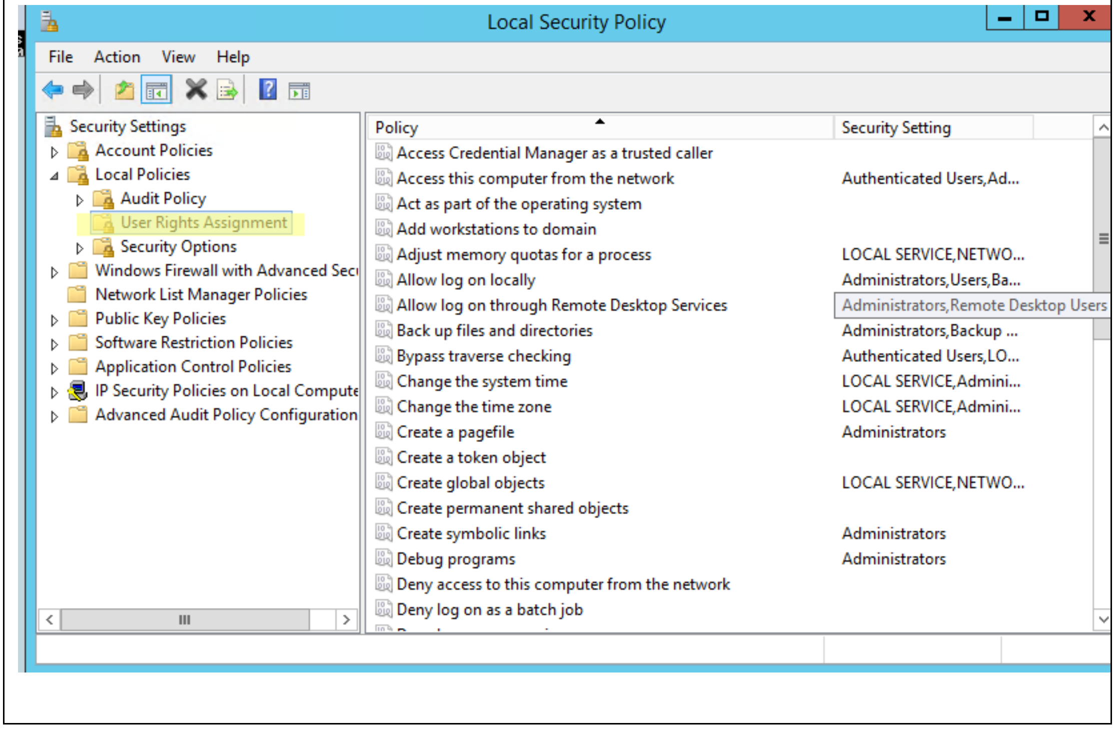
Click Local Security Policy



Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to

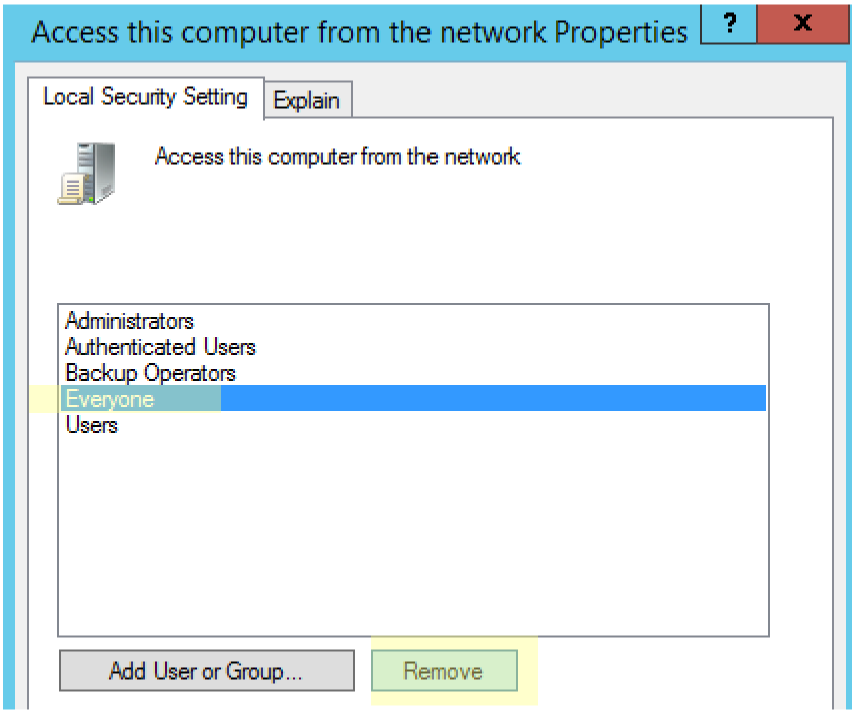
Security Settings – Local Policies – User Rights Assignment


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Authenticated Users,Ad...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Administrators,Users,Ba...
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Authenticated Users,LO...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	
Deny log on as a batch job	

Click Access this computer from the network

Remove Everyone

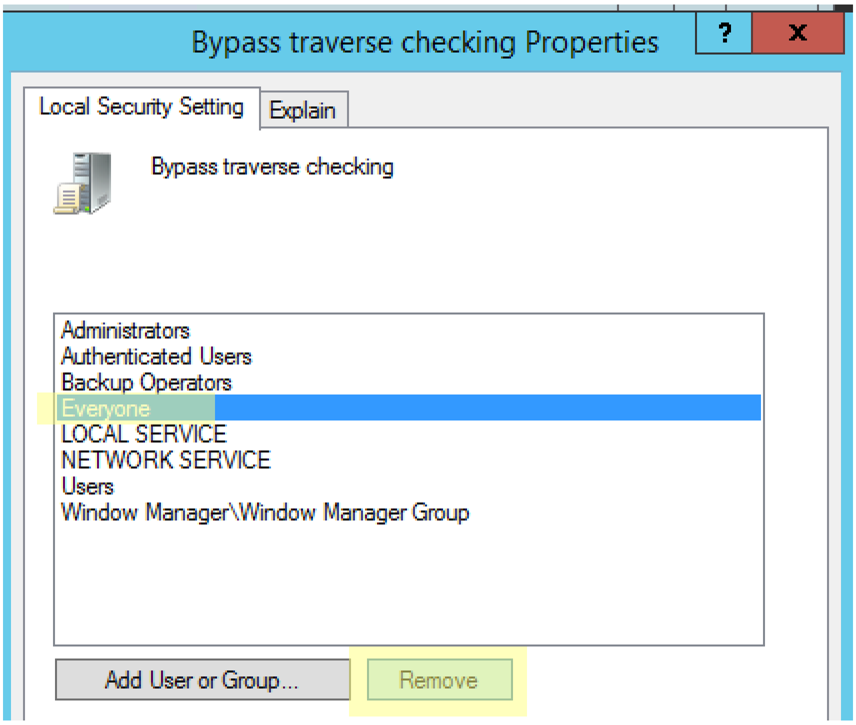


Access this computer from the network

Administrators
Authenticated Users
Backup Operators
Everyone
Users

Click Bypass traverse checking

Remove Everyone

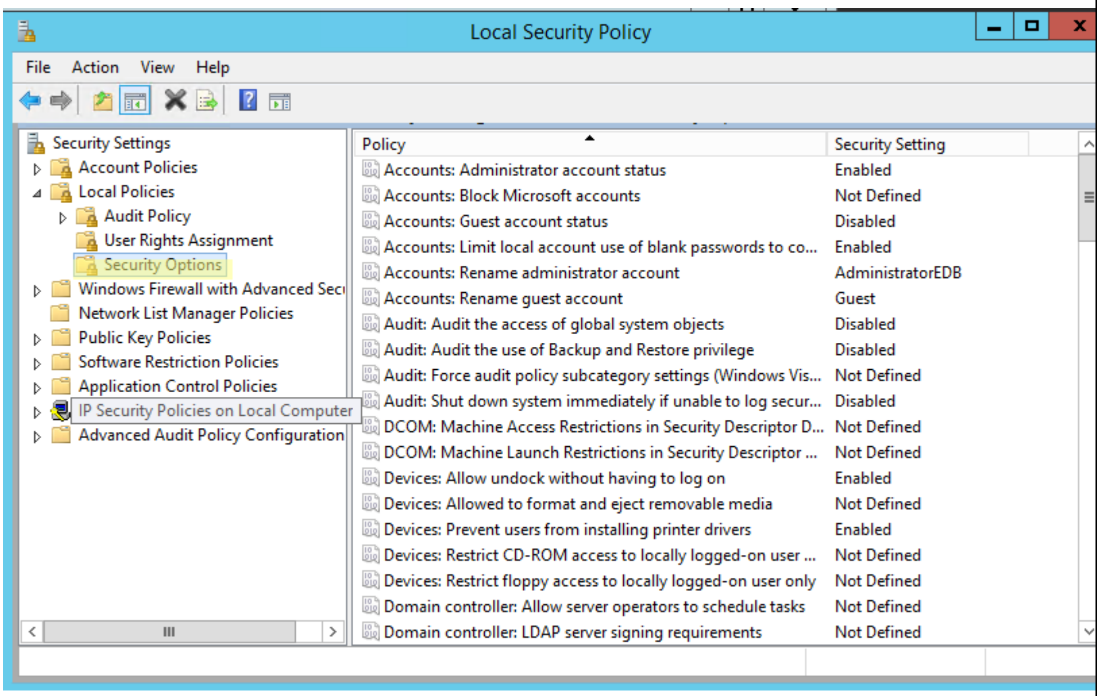


Bypass traverse checking

Administrators
Authenticated Users
Backup Operators
Everyone
LOCAL SERVICE
NETWORK SERVICE
Users
Window Manager\Window Manager Group

Navigate to

Security Settings – Local Policies – Security Options

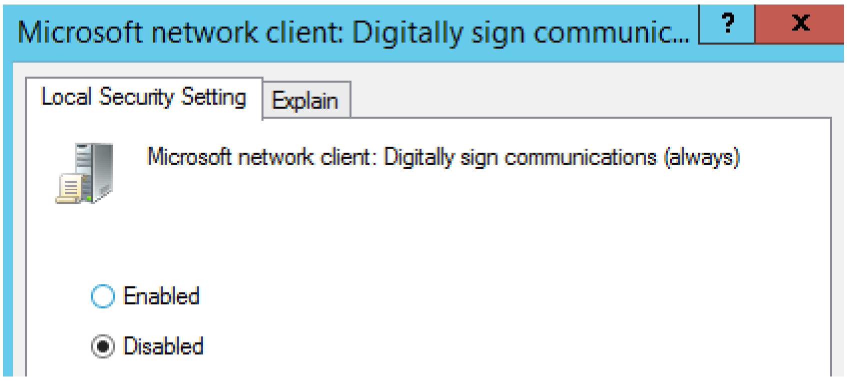


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	AdministratorEDB
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined

Click Microsoft network client : Digitally sign communications (always)

Select Disabled



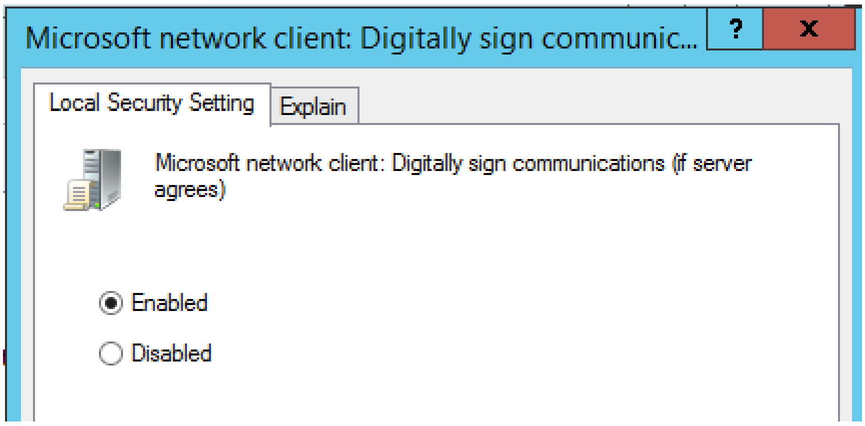
Microsoft network client: Digitally sign communications (always)

○ Enabled

● Disabled

Click Microsoft network client : Digitally sign communications (if server agrees)

Select Enabled



Microsoft network client: Digitally sign communic...

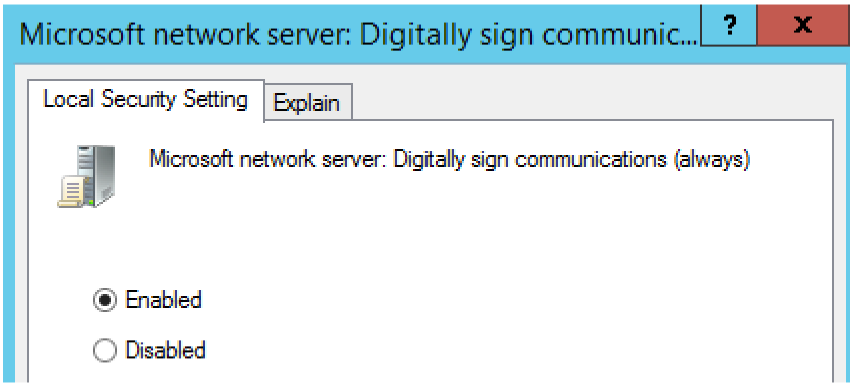
Microsoft network client: Digitally sign communications (if server agrees)

● Enabled

○ Disabled

Click Microsoft network server : Digitally sign communications (always)

Select Enabled



Microsoft network server: Digitally sign communic...

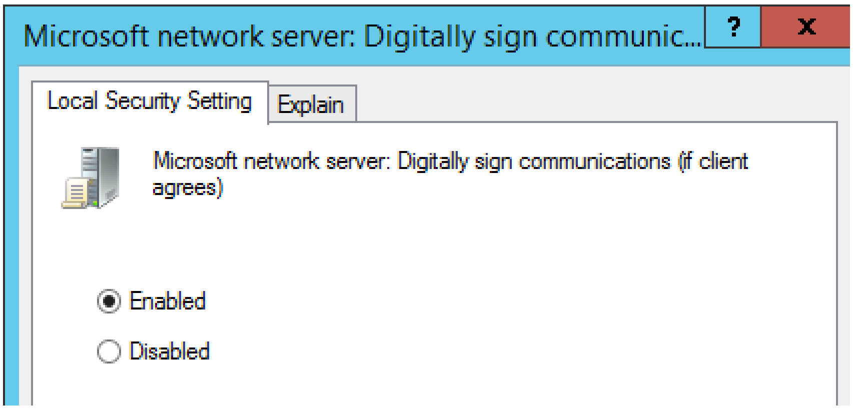
Microsoft network server: Digitally sign communications (always)

● Enabled

○ Disabled

Click Microsoft network server : Digitally sign communications (if client agrees)

Select Enabled



Microsoft network server: Digitally sign communic...

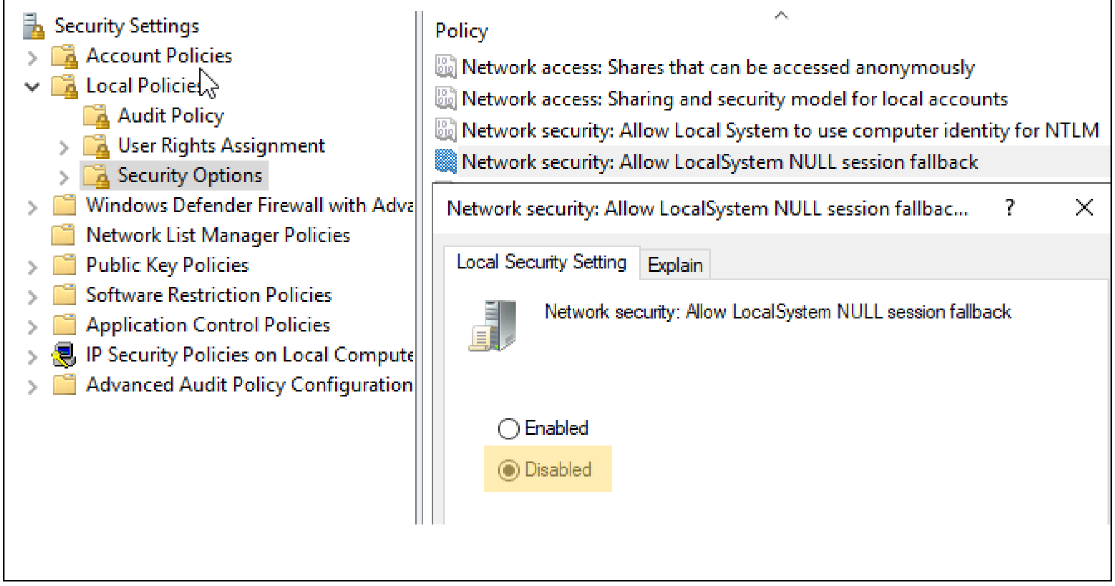
Microsoft network server: Digitally sign communications (if client agrees)

● Enabled

○ Disabled

Click network security : Allow LocalSystem NULL session fallback

Select Disabled


Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
?
Local Security Setting
Explain

Network access: Shares that can be accessed anonymously

Network access: Sharing and security model for local accounts

Network security: Allow Local System to use computer identity for NTLM

Network security: Allow LocalSystem NULL session fallback

Network security: Allow LocalSystem NULL session fallbac...

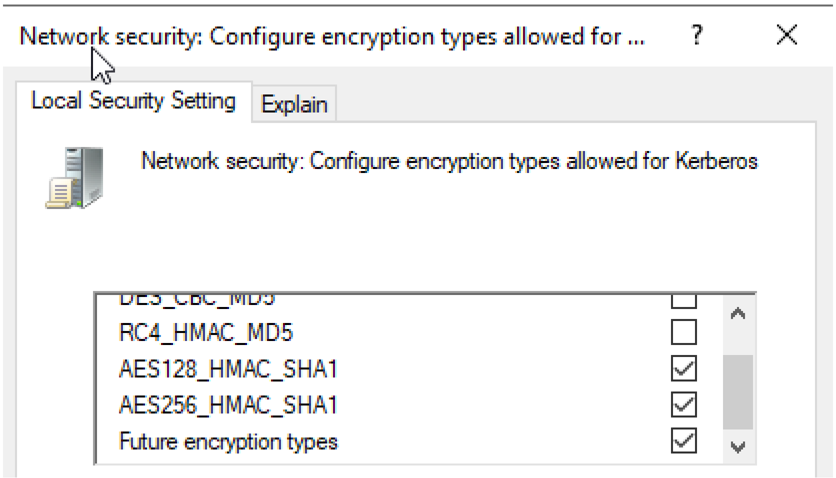
Network security: Allow LocalSystem NULL session fallback

○ Enabled

● Disabled

Click Network security: Configure encryption types allowed for Kerberos

Select AES128_HMAC_SHA1, AES256_HMAC_SHA1 and Future encryption types

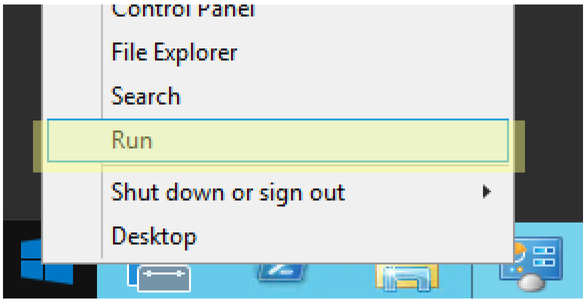


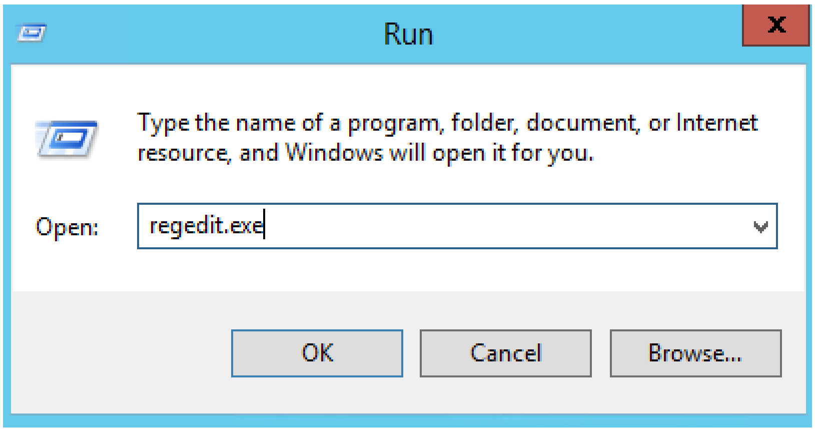
Network security: Configure encryption types allowed for ... ? ×

Network security: Configure encryption types allowed for Kerberos

- DES_CBC_MD5 □
- RC4_HMAC_MD5 □
- AES128_HMAC_SHA1 ☑
- AES256_HMAC_SHA1 ☑
- Future encryption types ☑

Run regedit.exe (registry editor)





Run

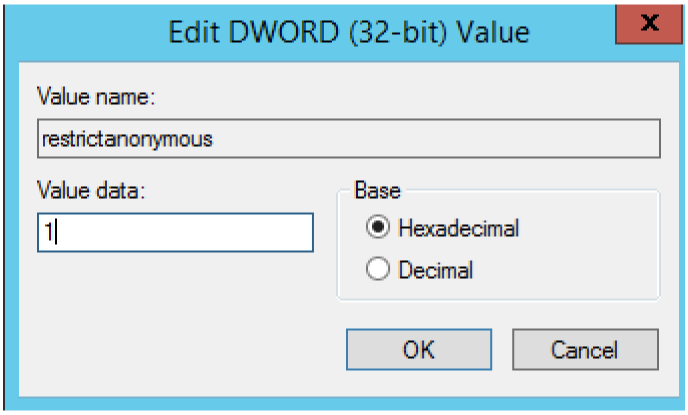
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit.exe

Navigate to

HKEY_LOCAL_MACHINE \SYSTEM\ CurrentControlSet\ Control\Lsa

Set restrictanonymous=1



Edit DWORD (32-bit) Value

Value name: restrictanonymous

Value data: 1

Base

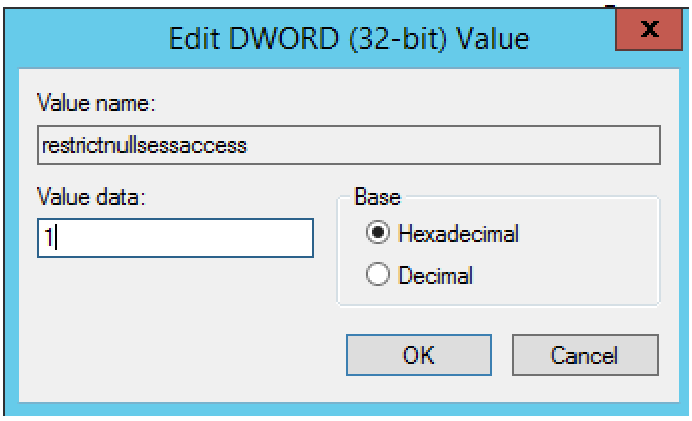
● Hexadecimal

○ Decimal

Navigate to

HKEY_LOCAL_MACHINE\
SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Set restrictnullsessaccess=1



Edit DWORD (32-bit) Value

Value name: restrictnullsessaccess

Value data: 1

Base

● Hexadecimal

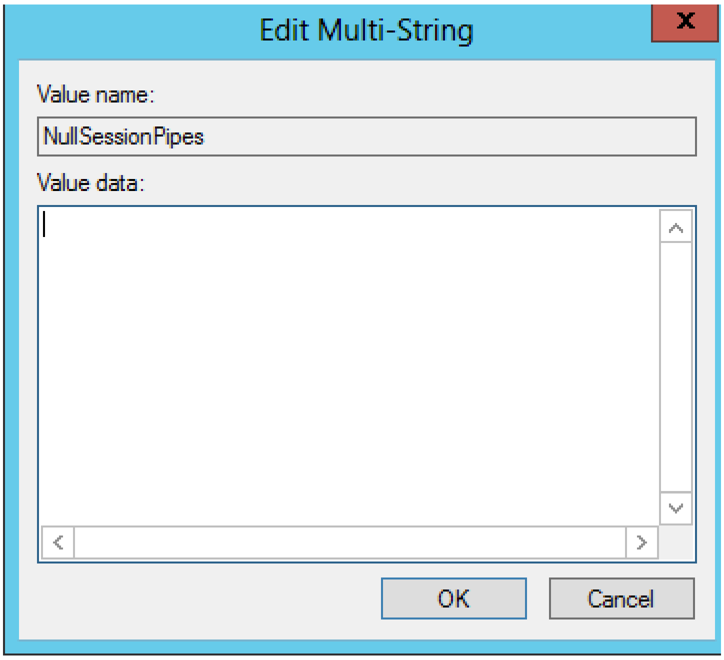
○ Decimal

Navigate to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

NullSessionPipes

Remove BROWSER if have

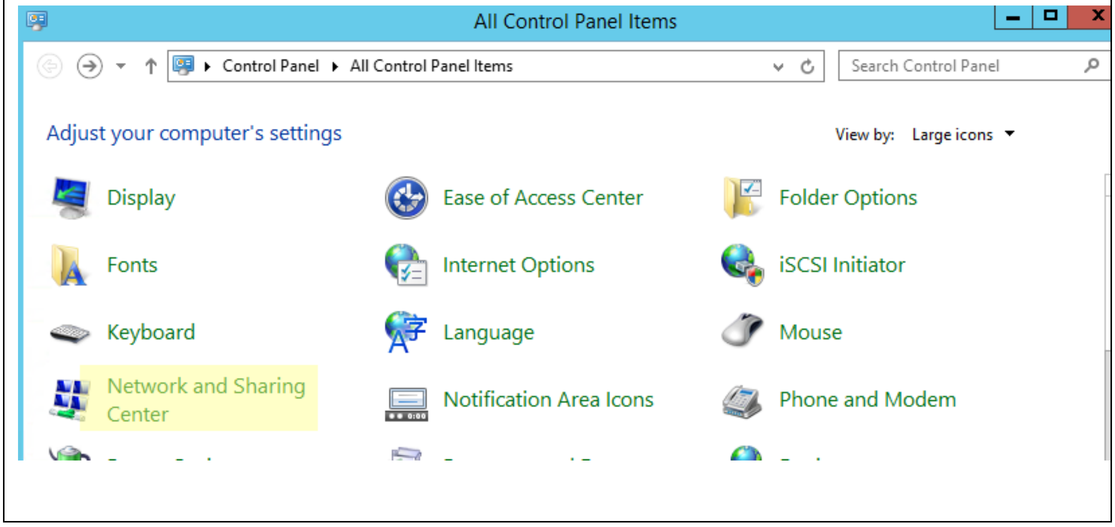


Edit Multi-String

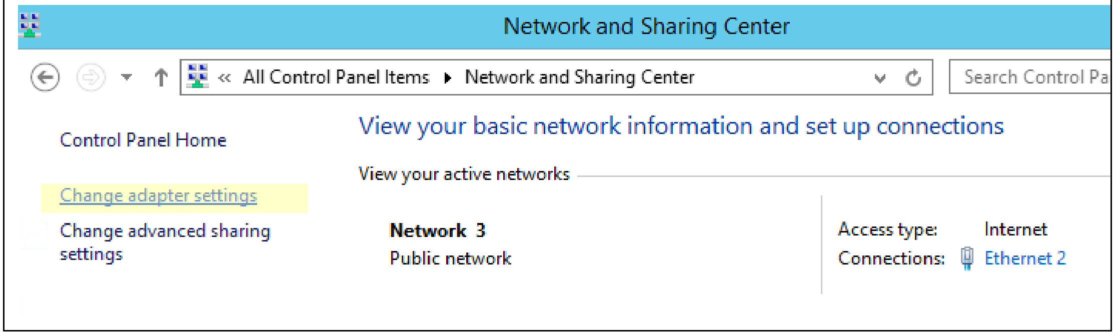
Value name: NullSessionPipes

Value data:

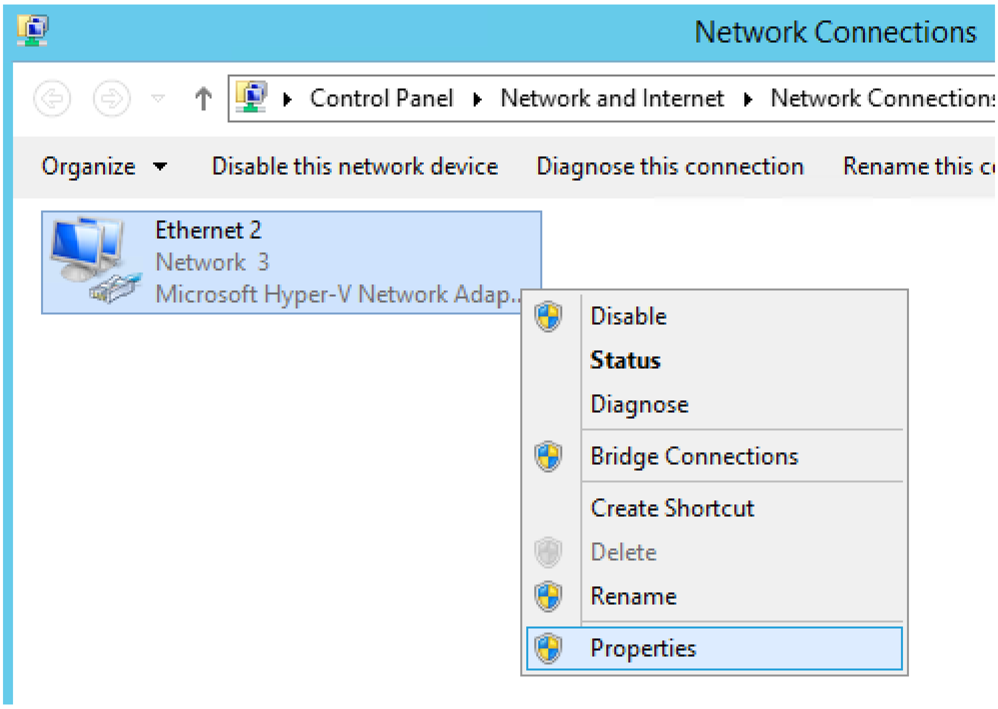
In All Control Panel Items, click Network and Sharing Center



Click Change adapter settings

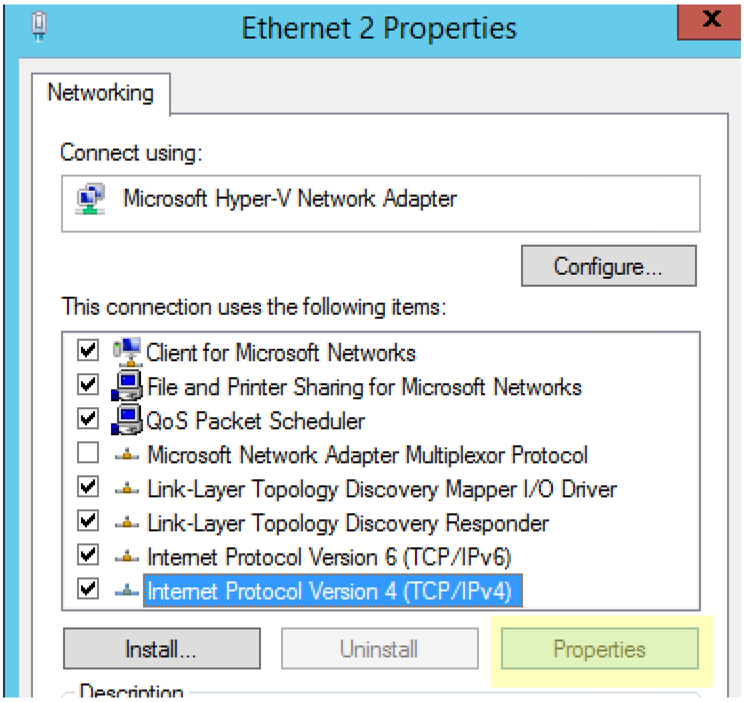

Network and Sharing Center
All Control Panel Items
Network and Sharing Center
Search Control Pa
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Network 3
Public network
Access type: Internet
Connections: Ethernet 2

Right click the Ethernet and click properties



Select Internet Protocol Version 4(TCP/IPv4)

Click Properties


Ethernet 2 Properties

Networking

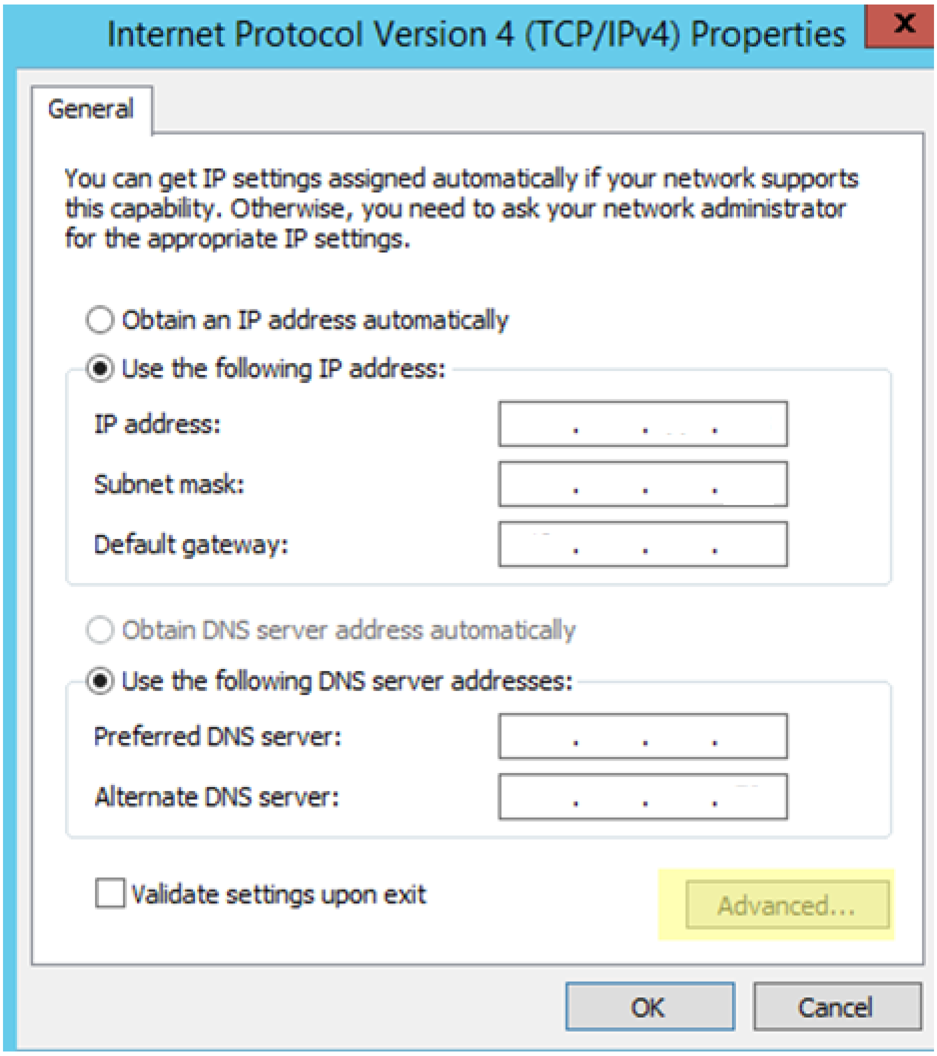
Connect using:

Microsoft Hyper-V Network Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Click Advanced



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

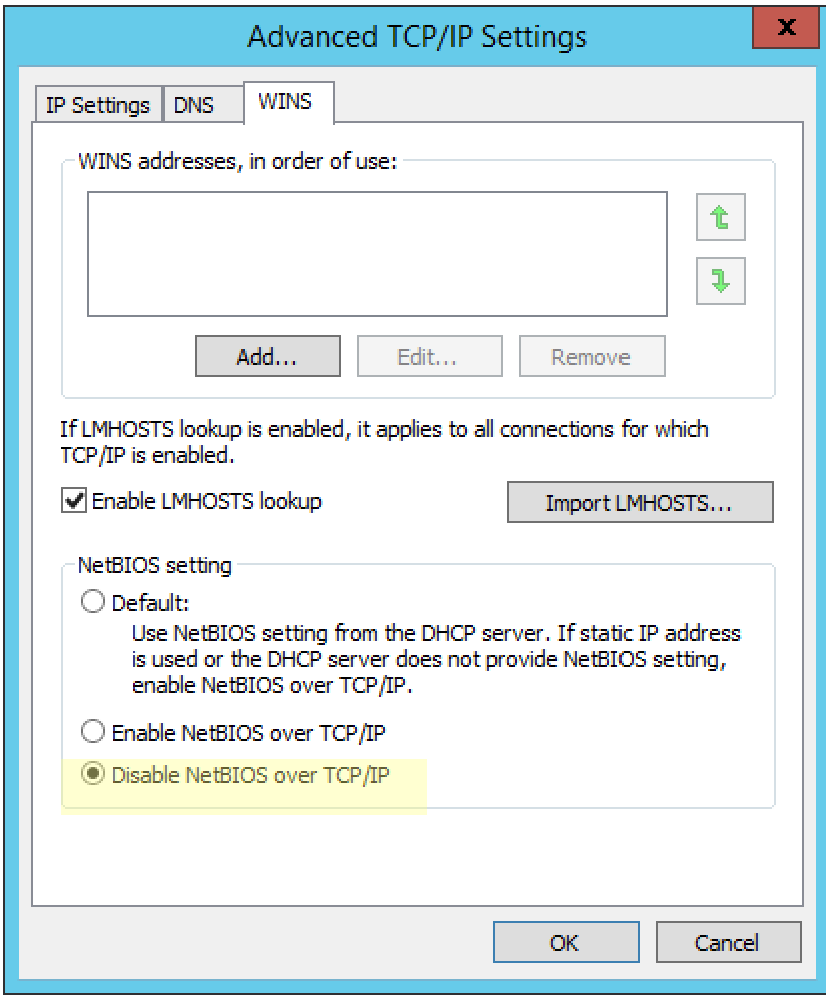
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Select Disable NetBIOS over TCP/IP



WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

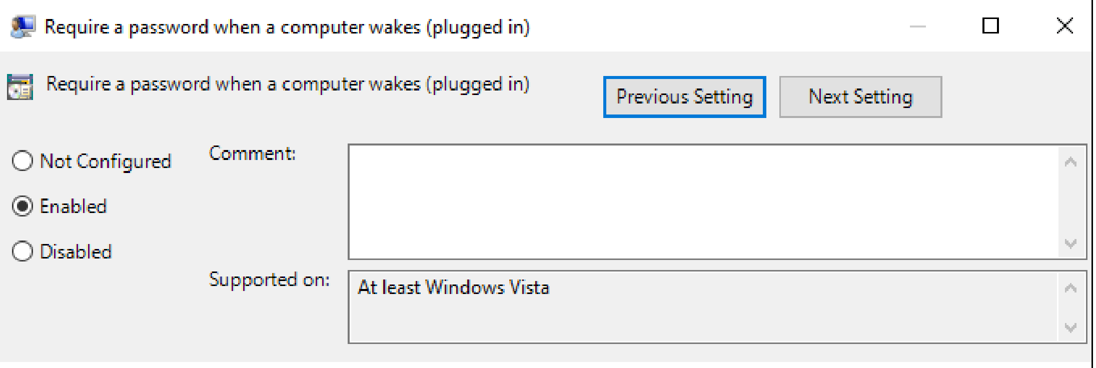
Run gpedit.msc

Navigate to

Computer Configuration – Administrative Templates – System – Power Management – Sleep Settings

Click Require a password when a computer wakes (plugged in)

Select Enabled



Require a password when a computer wakes (plugged in)

Require a password when a computer wakes (plugged in)

○ Not Configured
● Enabled
○ Disabled

Comment:

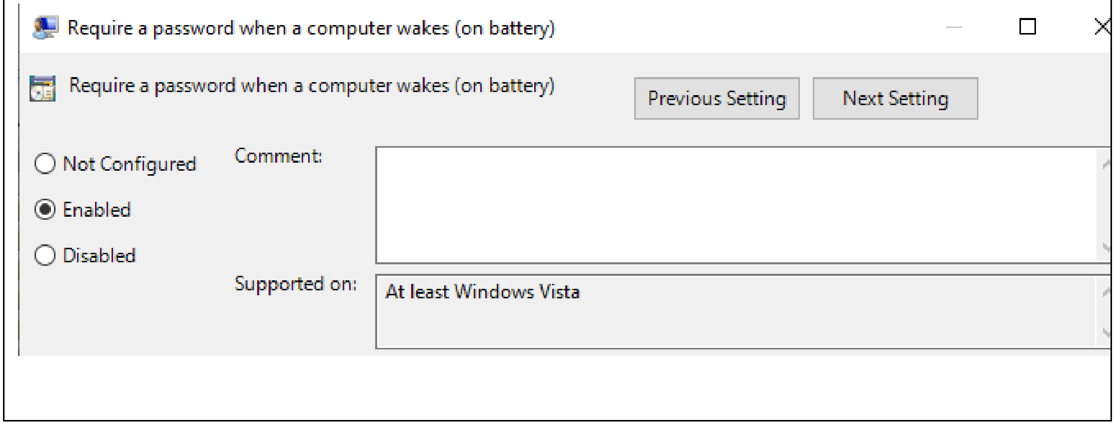
Supported on: At least Windows Vista

Navigate to

Computer Configuration – Administrative Templates – System – Power Management – Sleep Settings

Click Require a password when a computer wakes (on battery)

Select Enabled



Require a password when a computer wakes (on battery)

Require a password when a computer wakes (on battery)

○ Not Configured
● Enabled
○ Disabled

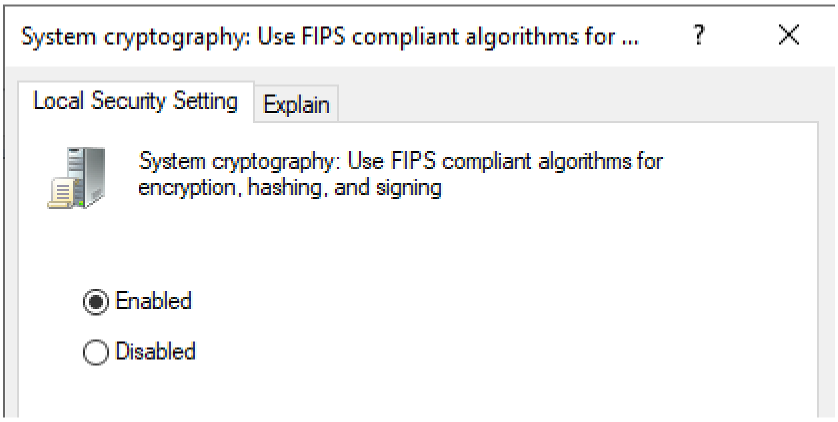
Comment:

Supported on: At least Windows Vista

Run gpedit.msc

Navigate to
Computer Configuration – Windows Settings – Security Settings – Local Policy – Security Options

Click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing
Select Enabled



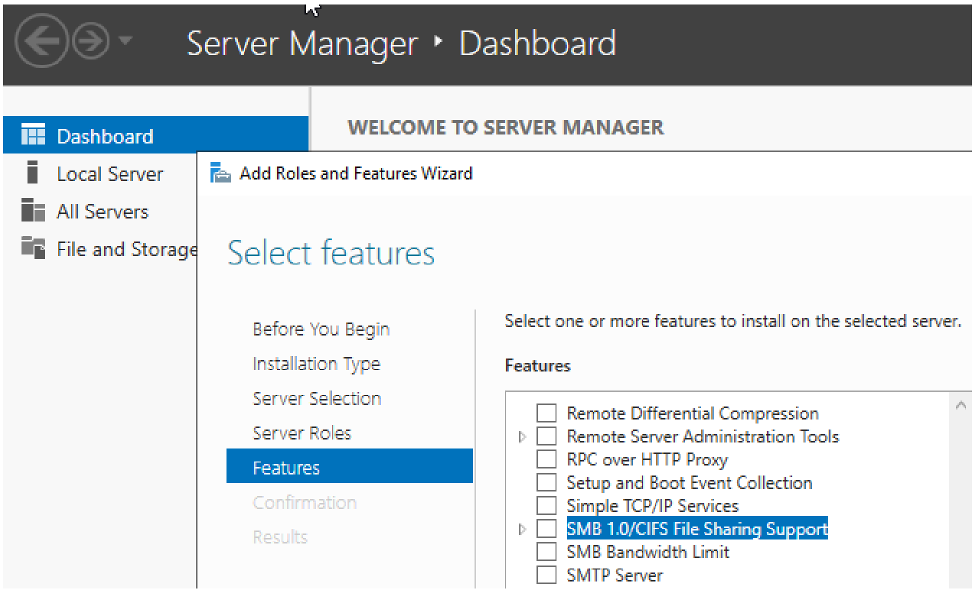
System cryptography: Use FIPS compliant algorithms for ...

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

● Enabled

○ Disabled

Go to Server Manager Dashboard
Deselect the SMB 1.0/CIFS File Sharing Support option



Server Manager ▸ Dashboard

Select features

Select one or more features to install on the selected server.

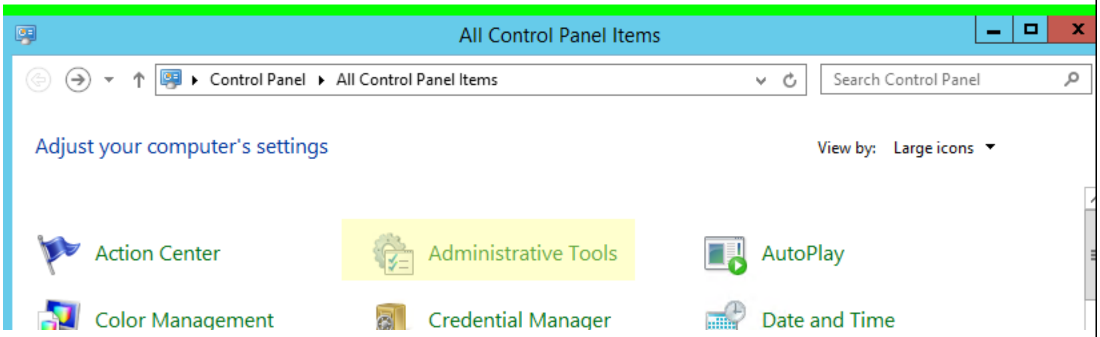
Features

- □ Remote Differential Compression
- □ Remote Server Administration Tools
- □ RPC over HTTP Proxy
- □ Setup and Boot Event Collection
- □ Simple TCP/IP Services
- □ SMB 1.0/CIFS File Sharing Support
- □ SMB Bandwidth Limit
- □ SMTP Server

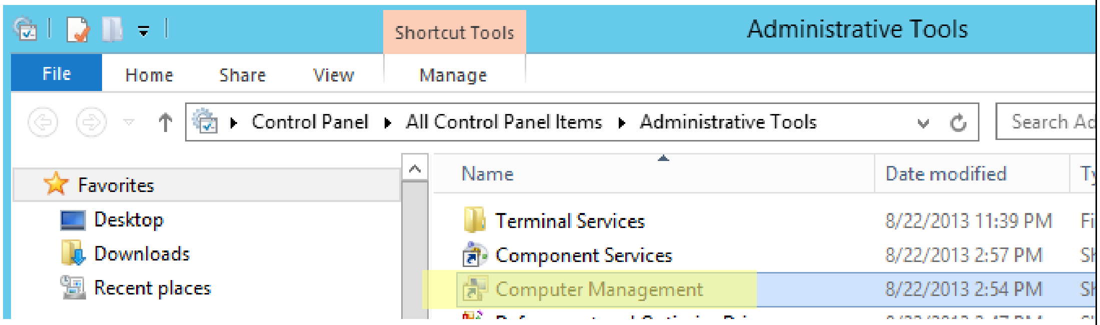
2.2 Account Security

2.2.1 User Account and Rights

In All Control Panel Items , click Administrative Tools



Click Computer Management

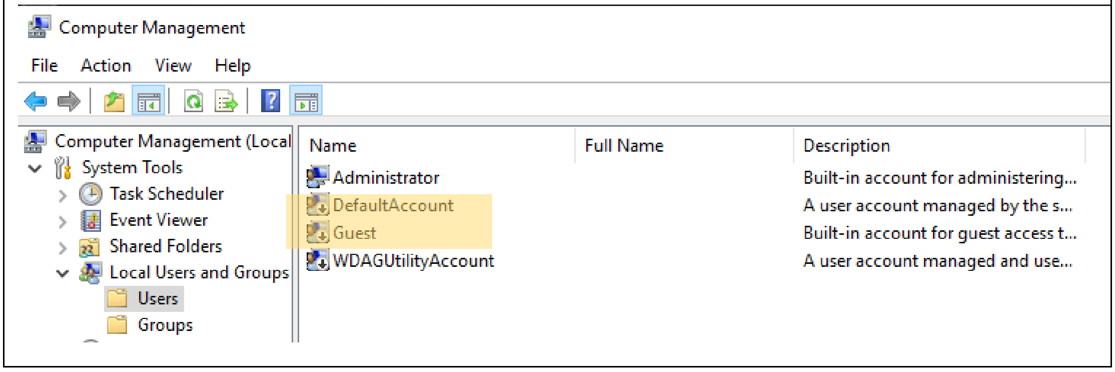


Name	Date modified
Terminal Services	8/22/2013 11:39 PM
Component Services	8/22/2013 2:57 PM
Computer Management	8/22/2013 2:54 PM

Click Local Users and Groups and Users

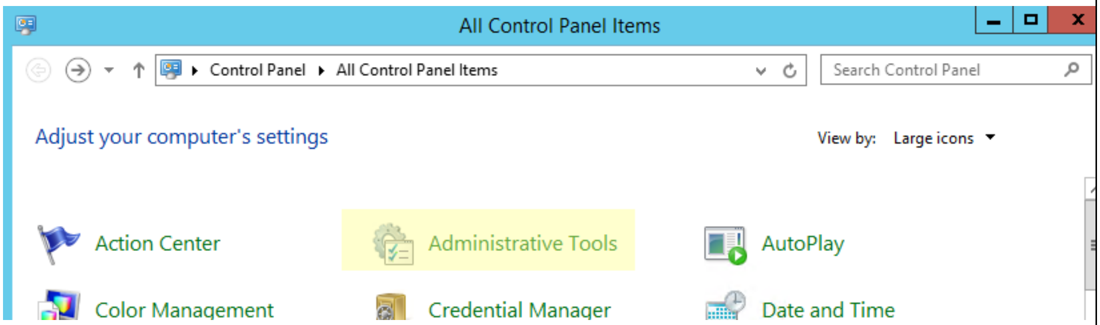
Disable or remove any unused accounts, such as DefaultAccount and Guest etc.

It is not recommended to use a default administrator account name, such as "administrator" or "admin". You may either rename the default administrator account or create an account and set it as an administrative account.

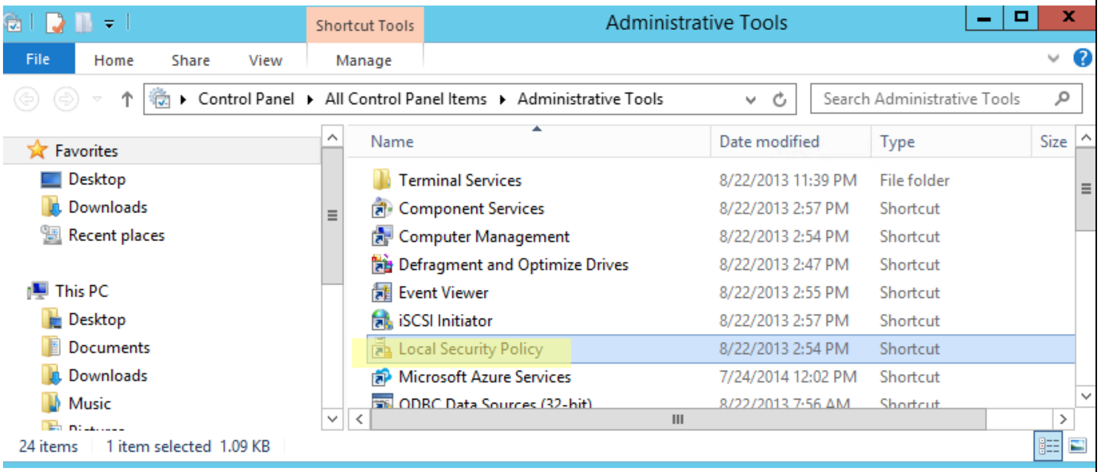


Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAccount		A user account managed by the s...
Guest		Built-in account for guest access t...
WDAGUtilityAccount		A user account managed and use...

In All Control Panel Items , click Administrative Tools



Click Local Security Policy

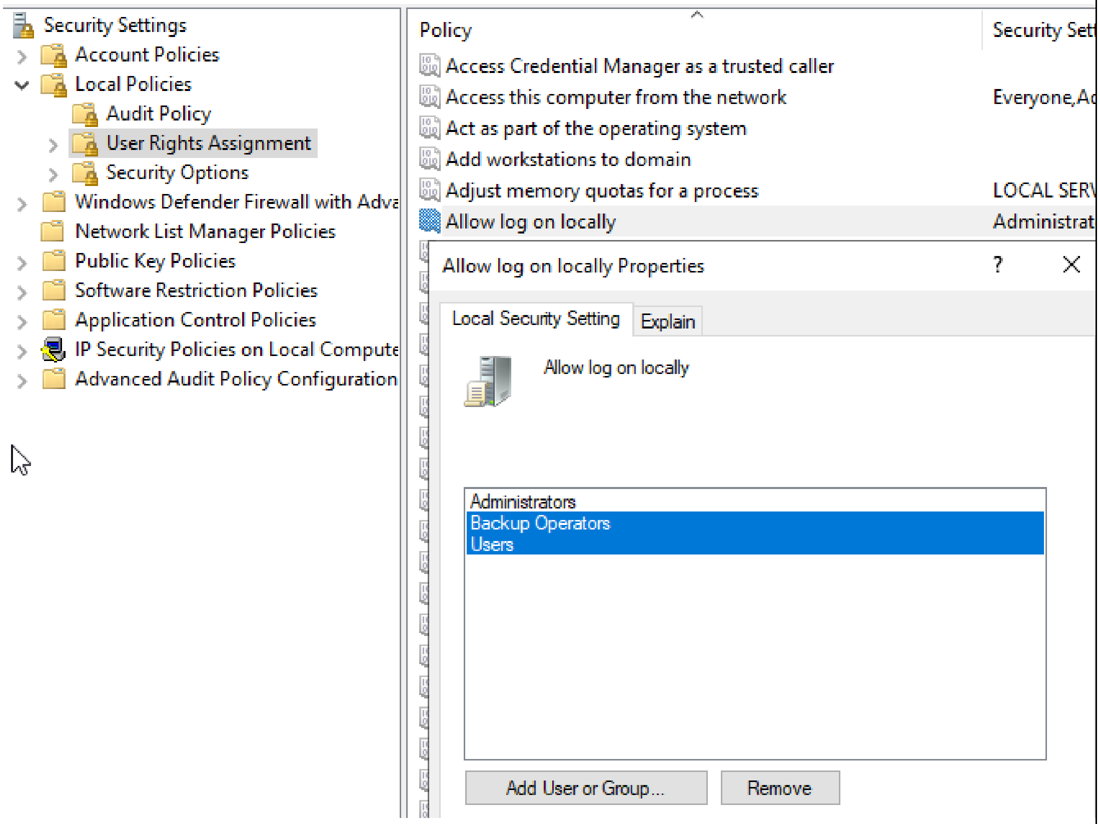


Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to

Local Policies-User Rights Assignment

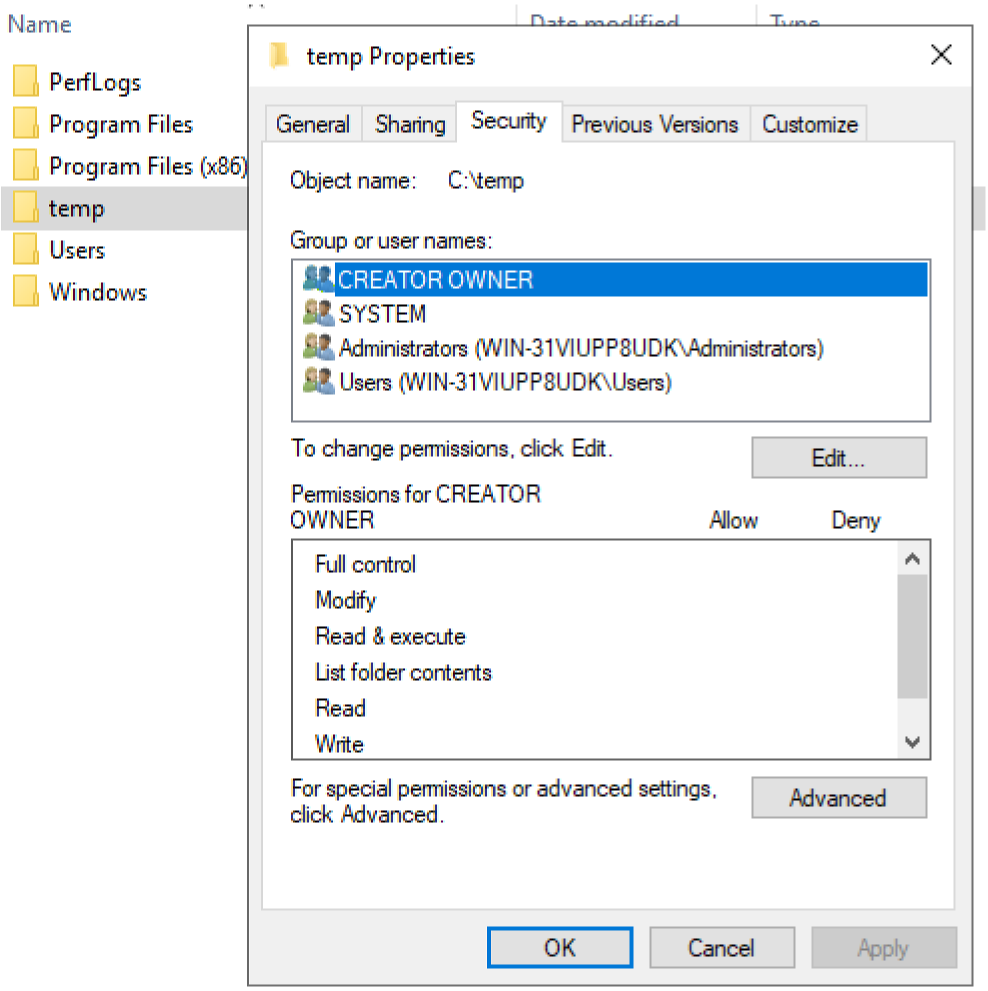
Click Allow log on locally, remove all groups except Administrators, you may add your administrative account(s) to this group.


Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Sett
Access Credential Manager as a trusted caller
Access this computer from the network
Everyone,Ad
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
LOCAL SERV
Allow log on locally
Administrat
Allow log on locally Properties
?
Local Security Setting
Explain
Allow log on locally
Add User or Group...
Remove

Administrators
Backup Operators
Users

Reminders:

- ✓ Full permissions should NOT be granted to everyone or guest group in the configuration of file or folder.
- ✓ Sharing should NOT be allowed for anonymous access.
- ✓ The principle of least privilege (POLP) should always be strictly executed.



Object name: C:\temp

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (WIN-31VIUPP8UDK\Administrators)
- Users (WIN-31VIUPP8UDK\Users)

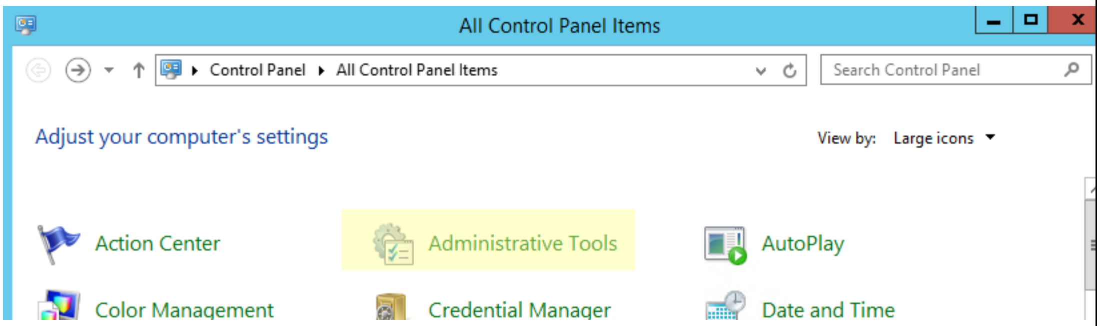
To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

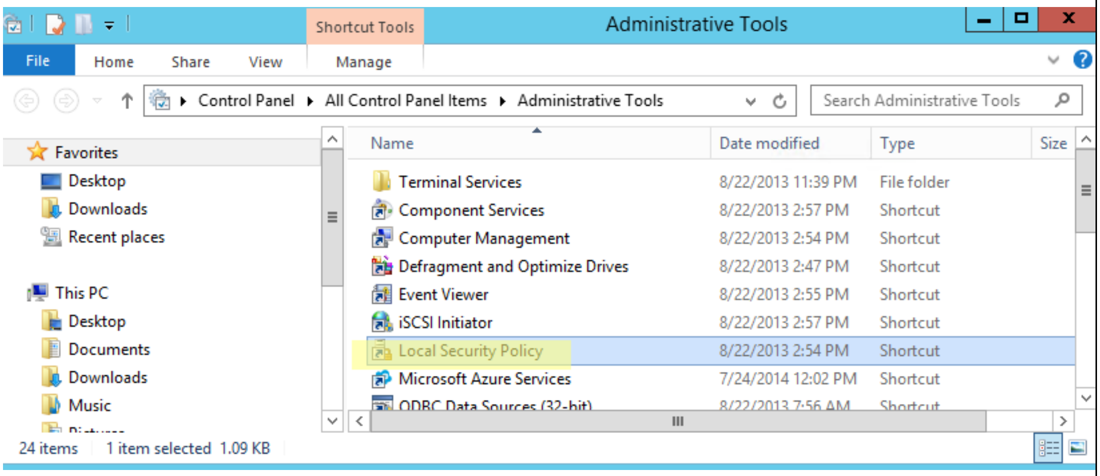
For special permissions or advanced settings, click Advanced.

2.2.2 Password Policy

In All Control Panel Items , click Administrative Tools



Click Local Security Policy



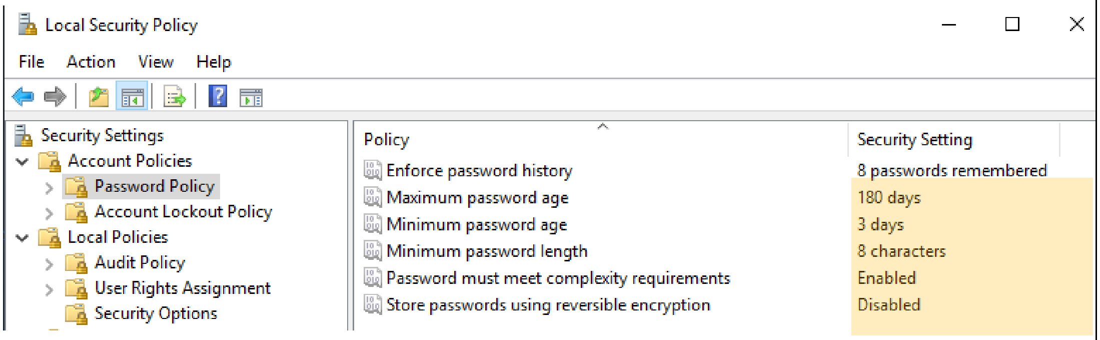
Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to

Security Settings – Account Policies – Password Policy

Policy	Security Setting
Enforce password history	8 passwords remembered
Maximum password age	180 days
Minimum password age	3 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

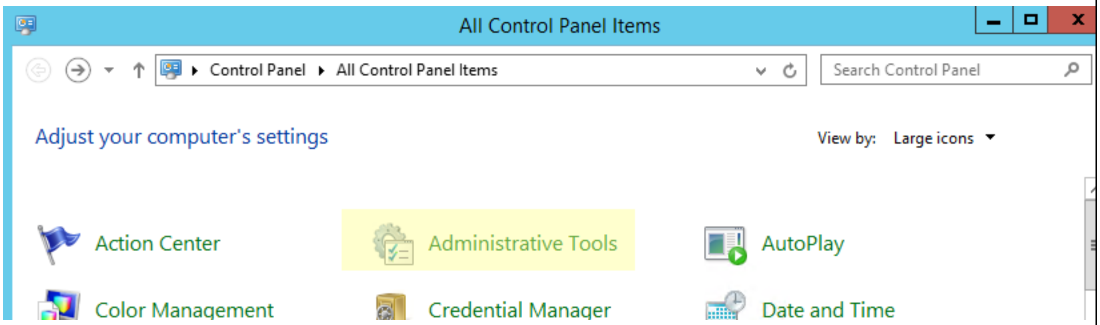
Result is



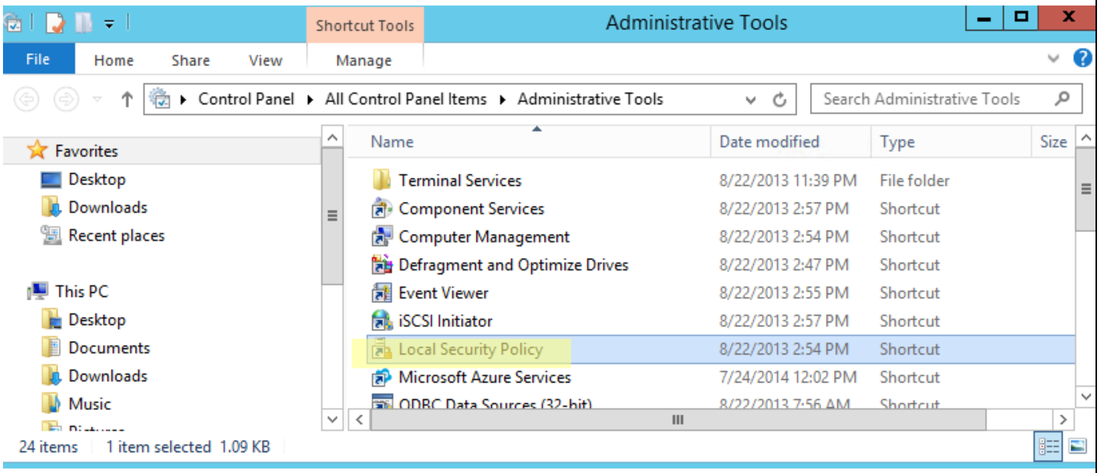
Policy	Security Setting
Enforce password history	8 passwords remembered
Maximum password age	180 days
Minimum password age	3 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

2.2.3 Account Lockout Policy

In All Control Panel Items , click Administrative Tools



Click Local Security Policy



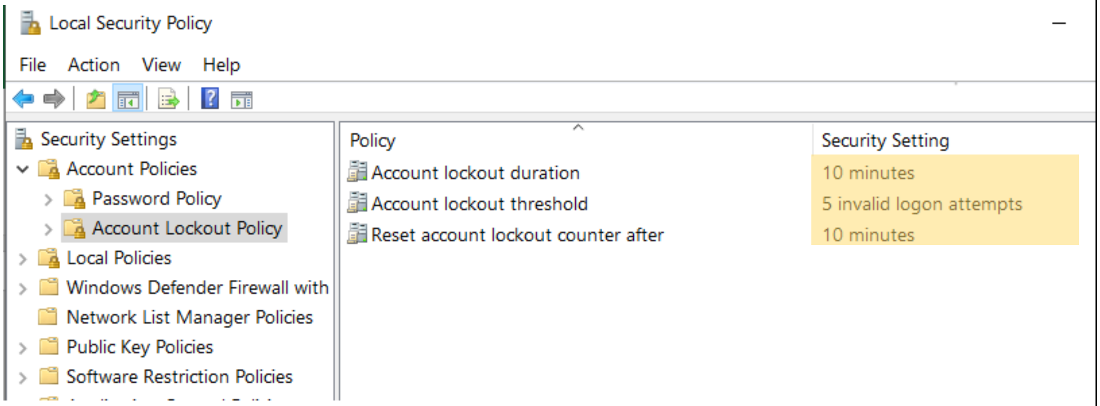
Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to

Security Settings – Account Policies – Account Lockout Policy

Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	10 minutes

Result is

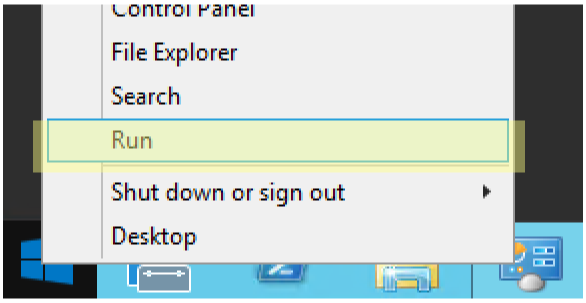


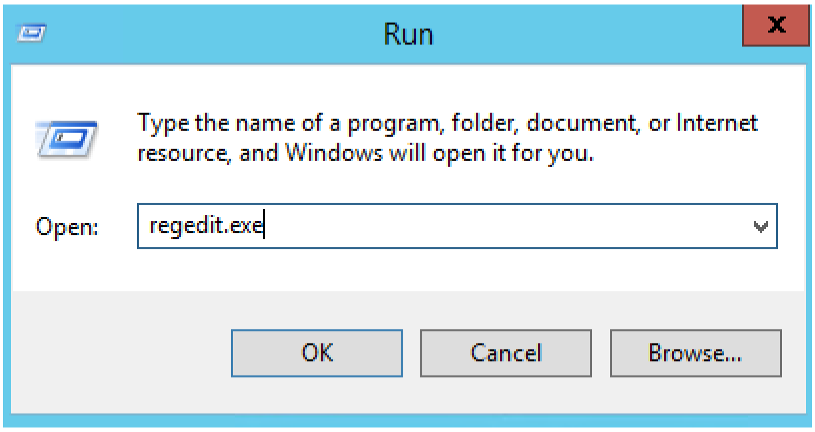
- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Defender Firewall with
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies

Policy	Security Setting
Account lockout duration	10 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	10 minutes

2.2.4 Screen Saver

Run regedit.exe (registry editor)



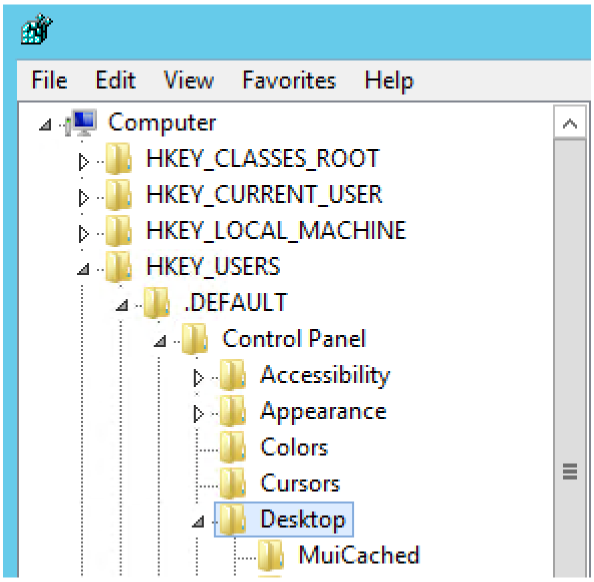


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

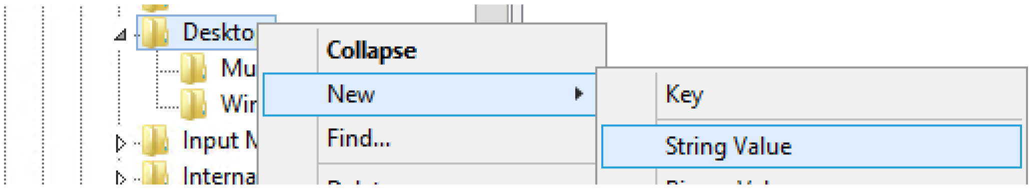
Open: regedit.exe

Navigate to

HKEY_USERS – .DEFAULT – Control Panel – Desktop

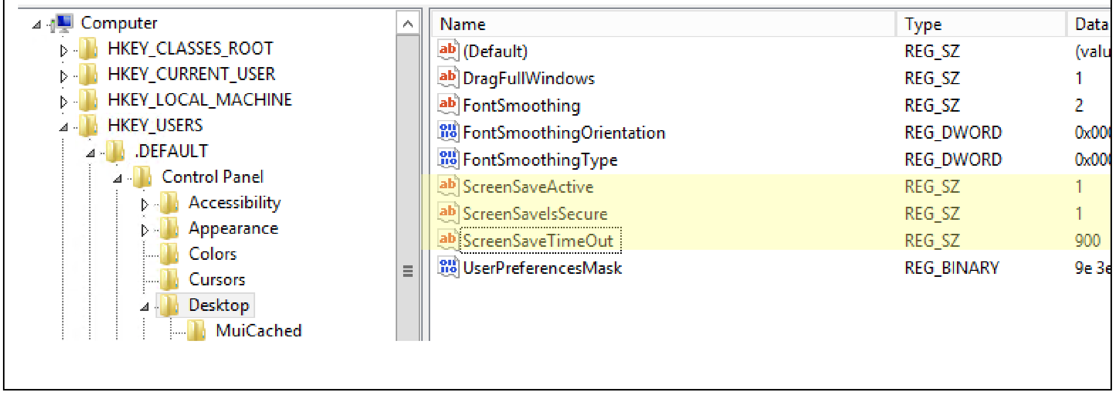


Right click to add new String Value as



ScreenSaveActive	1
ScreenSaveIsSecure	1
ScreenSaveTimeOut	900

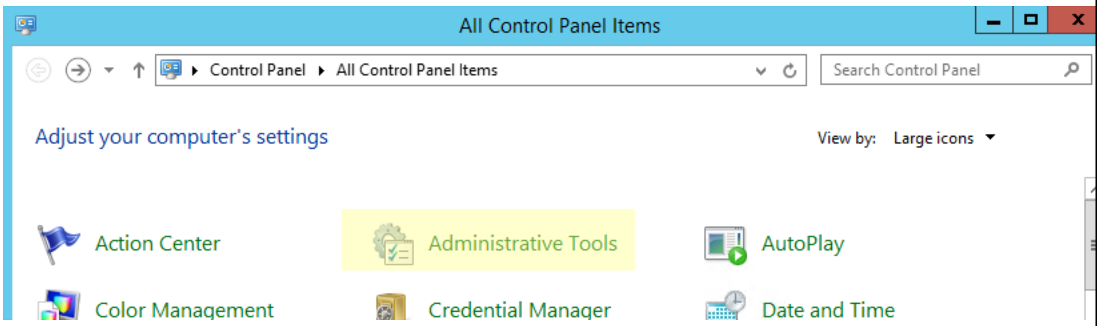
Result is



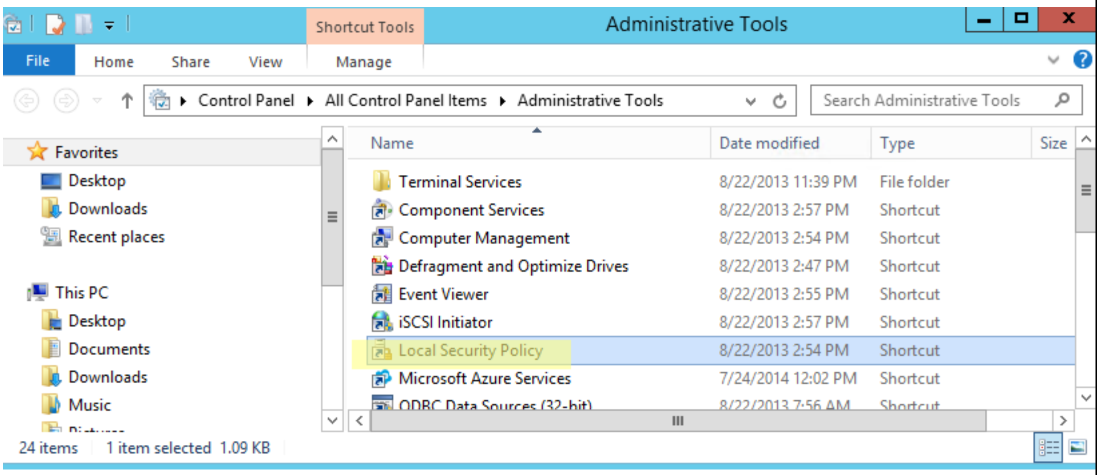
Name	Type	Data
(Default)	REG_SZ	(valu
DragFullWindows	REG_SZ	1
FontSmoothing	REG_SZ	2
FontSmoothingOrientation	REG_DWORD	0x00(
FontSmoothingType	REG_DWORD	0x00(
ScreenSaveActive	REG_SZ	1
ScreenSaveIsSecure	REG_SZ	1
ScreenSaveTimeOut	REG_SZ	900
UserPreferencesMask	REG_BINARY	9e 3e

2.3 Local Security Policy

In All Control Panel Items , click Administrative Tools

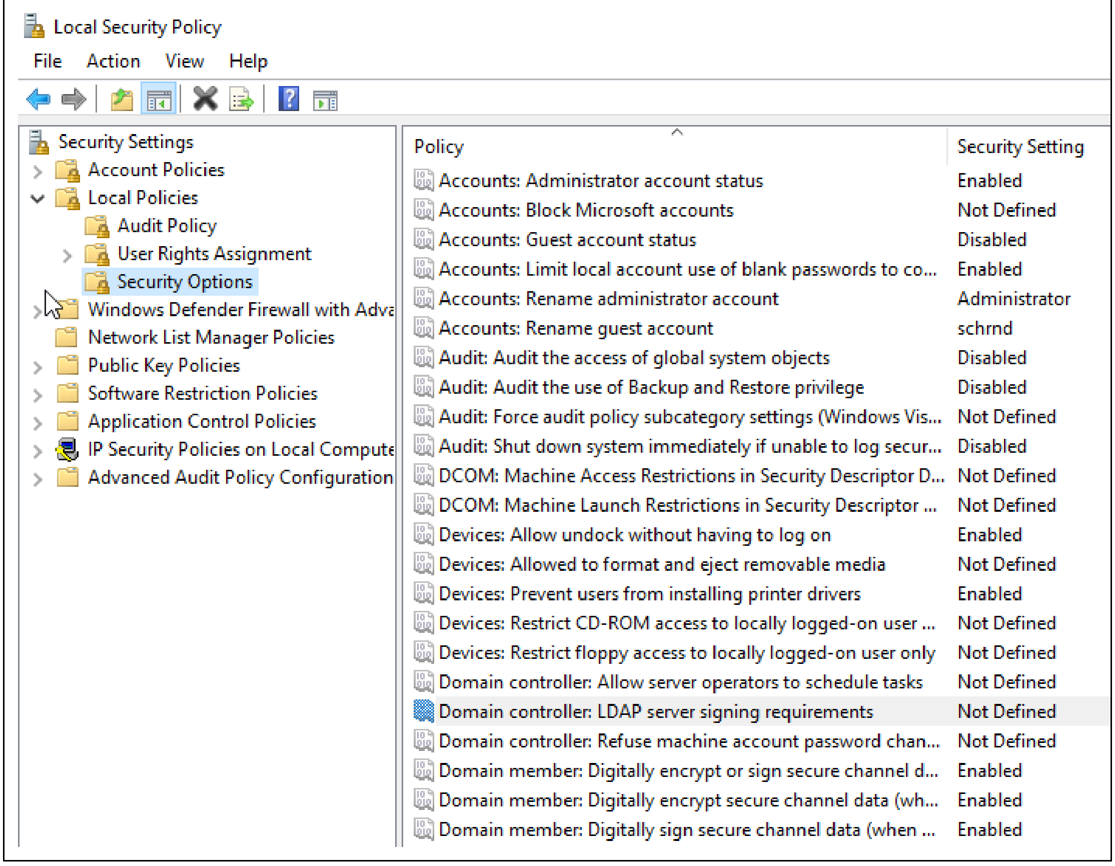


Click Local Security Policy



Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to Local Policies-Security Options


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	schrnd
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled

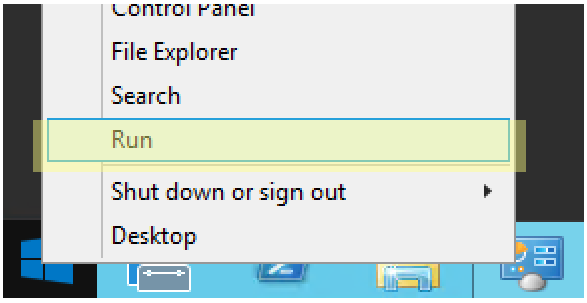
Set the additional Security Options by referring below table.

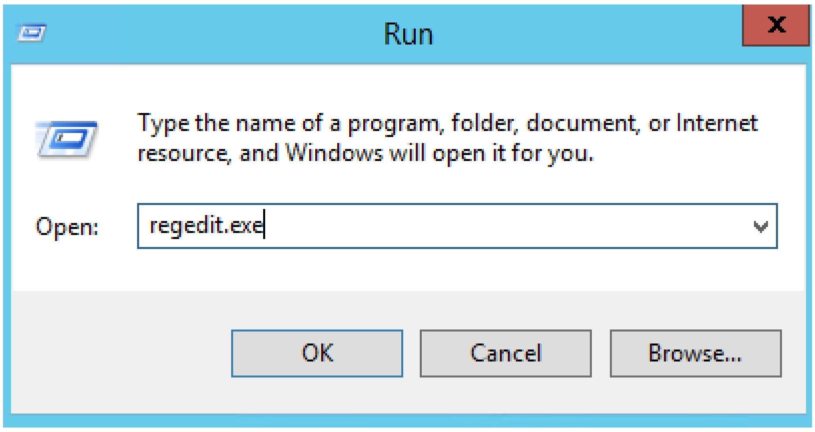
Policy	**Security Setting**
Accounts: Guest account status	Disabled
Accounts: Rename guest account	Assign any name other than the default name such as schrnd
Audit: Shut down system immediately if unable to log security audits	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (When possible)	Enabled
Interactive logon: Do not display username at sign-in	Enabled
Interactive logon: Message text for	“Authenticated User Only”

users attempting to log on	
Interactive logon: Message title for users attempting to log on	“Authenticated User Only”
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 logons
Interactive logon: Prompt user to change password before expiration	5 days
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled

2.4 Registry Security Configuration

1. Run regedit.exe (registry editor)





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit.exe

2. Navigate to [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]

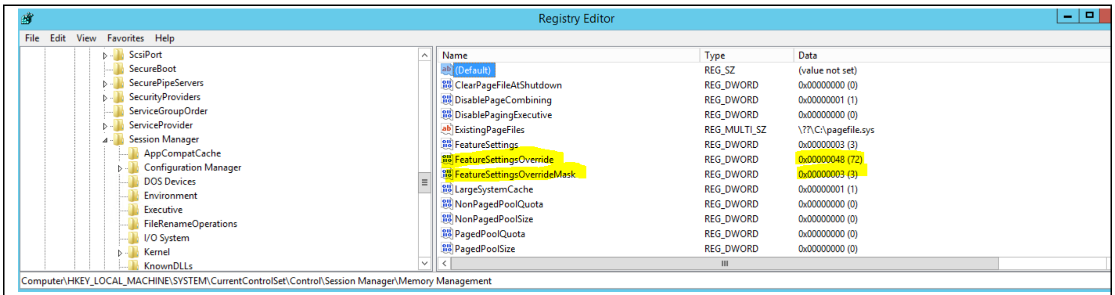
3. Configure the following Dwords

If Hyper-Threading enabled

"FeatureSettingsOverride"=dword:00000048
"FeatureSettingsOverrideMask"=dword:00000003

If Hyper-Threading disabled

"FeatureSettingsOverride"=dword:00002048
"FeatureSettingsOverrideMask"=dword:00000003

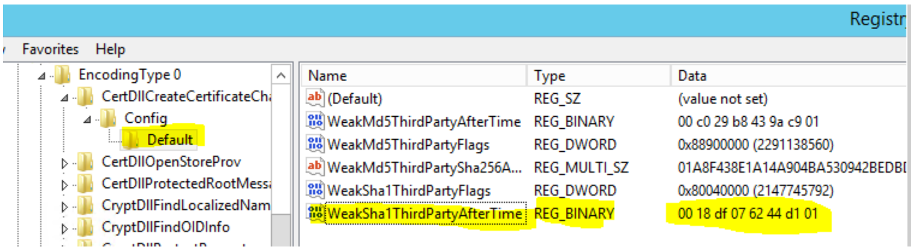


Name	Type	Data
(Default)	REG_SZ	(value not set)
ClearPageFileAtShutdown	REG_DWORD	0x00000000 (0)
DisablePageCombining	REG_DWORD	0x00000001 (1)
DisablePagingExecutive	REG_DWORD	0x00000000 (0)
ExistingPageFiles	REG_MULTI_SZ	\??\C:\pagefile.sys
FeatureSettings	REG_DWORD	0x00000003 (3)
FeatureSettingsOverride	REG_DWORD	0x00000048 (72)
FeatureSettingsOverrideMask	REG_DWORD	0x00000003 (3)
LargeSystemCache	REG_DWORD	0x00000001 (1)
NonPagedPoolQuota	REG_DWORD	0x00000000 (0)
NonPagedPoolSize	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

4. Navigate to [HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\default]

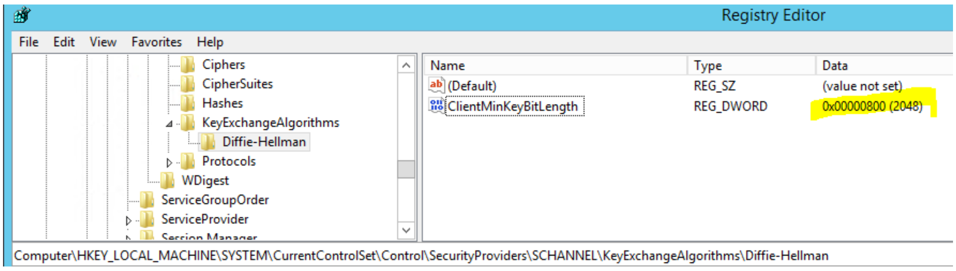
5. Configure the following <u>binary value</u> "WeakSha1ThirdPartyAfterTime"=0018df076244d101



Name	Type	Data
(Default)	REG_SZ	(value not set)
WeakMd5ThirdPartyAfterTime	REG_BINARY	00 c0 29 b8 43 9a c9 01
WeakMd5ThirdPartyFlags	REG_DWORD	0x88900000 (2291138560)
WeakMd5ThirdPartySha256A...	REG_MULTI_SZ	01A8F438E1A14A904BA530942BEDB
WeakSha1ThirdPartyFlags	REG_DWORD	0x80040000 (2147745792)
WeakSha1ThirdPartyAfterTime	REG_BINARY	00 18 df 07 62 44 d1 01

6. Navigate to [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

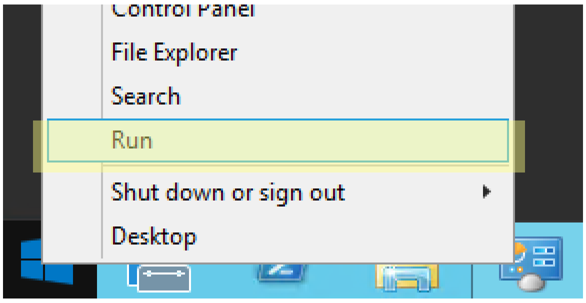
7. Configure the following Dword "ClientMinKeyBitLength"=dword: 00000800

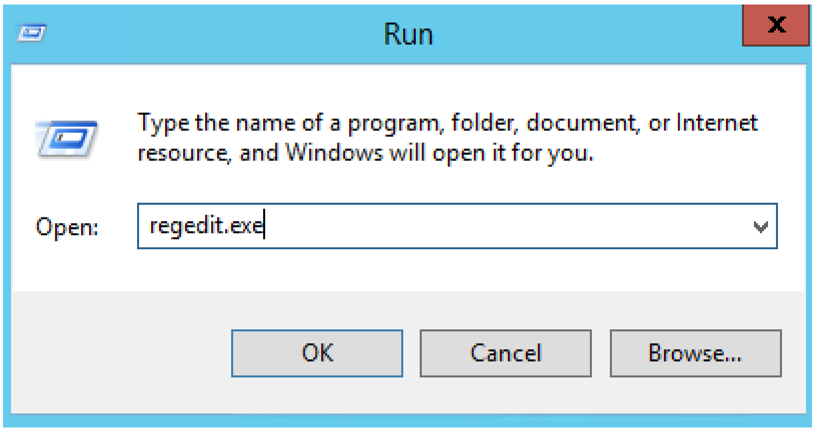


Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientMinKeyBitLength	REG_DWORD	0x00000800 (2048)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman

Run regedit.exe (registry editor)





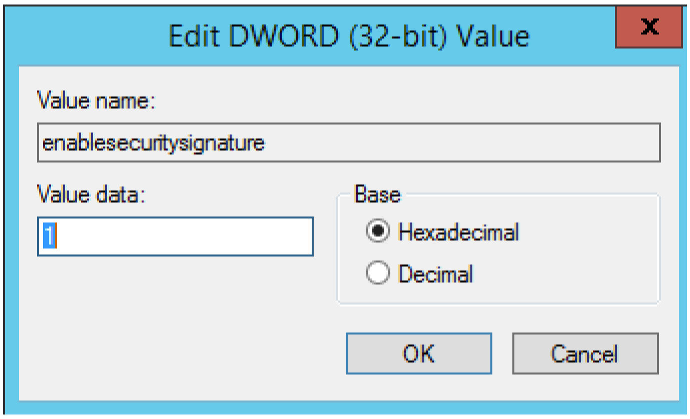
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit.exe

Navigate to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\ Parameters

Change enablesecuritysignature to 1

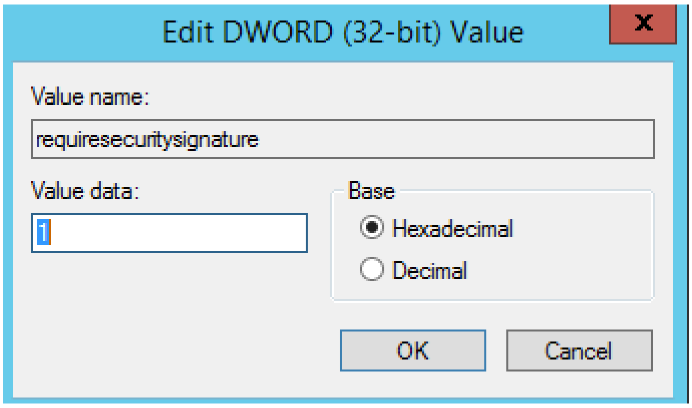


Value name: enablesecuritysignature

Value data: 1

Base
● Hexadecimal
○ Decimal

Change requiresecuritysignature to 1



Edit DWORD (32-bit) Value

Value name: requiresecuritysignature

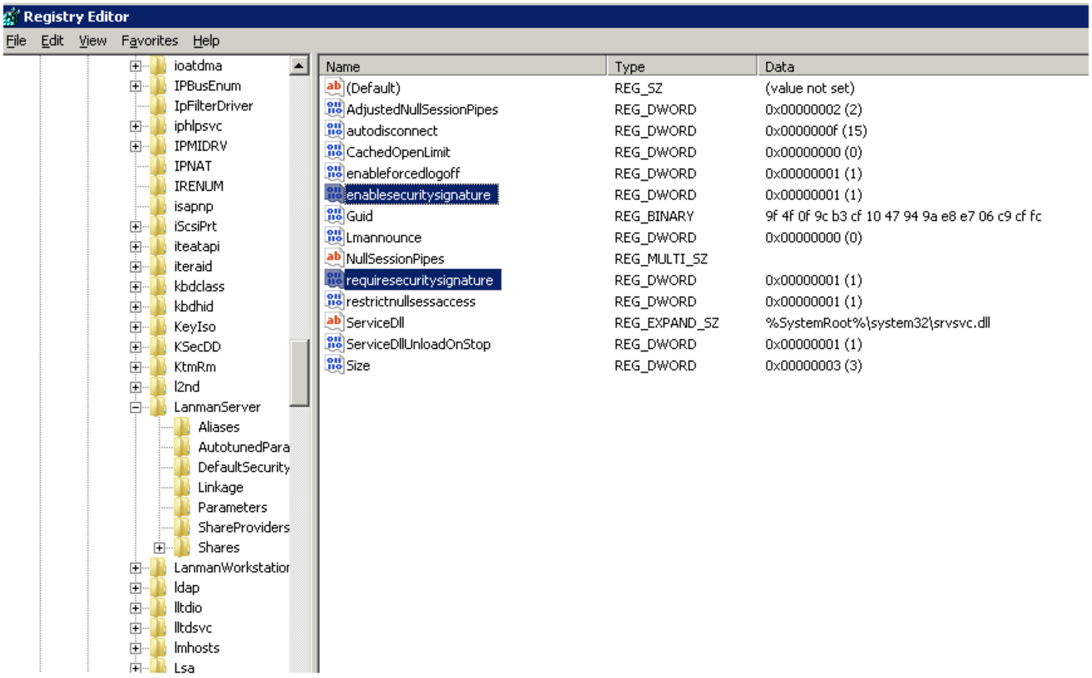
Value data: 1

Base

● Hexadecimal

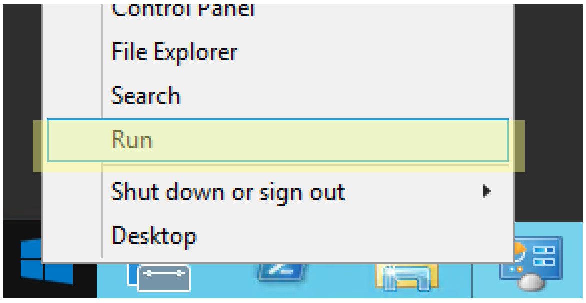
○ Decimal

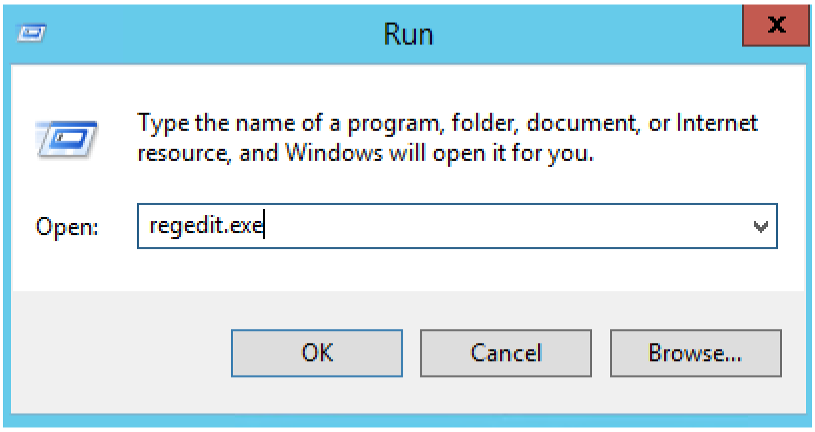
Result is



Name	Type	Data
(Default)	REG_SZ	(value not set)
AdjustedNullSessionPipes	REG_DWORD	0x00000002 (2)
autodisconnect	REG_DWORD	0x0000000f (15)
CachedOpenLimit	REG_DWORD	0x00000000 (0)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000001 (1)
Guid	REG_BINARY	9f 4f 0f 9c b3 cf 10 47 94 9a e8 e7 06 c9 cf fc
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	
requiresecuritysignature	REG_DWORD	0x00000001 (1)
restrictnullsessaccess	REG_DWORD	0x00000001 (1)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\srvsvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
Size	REG_DWORD	0x00000003 (3)

Run regedit.exe (registry editor)





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

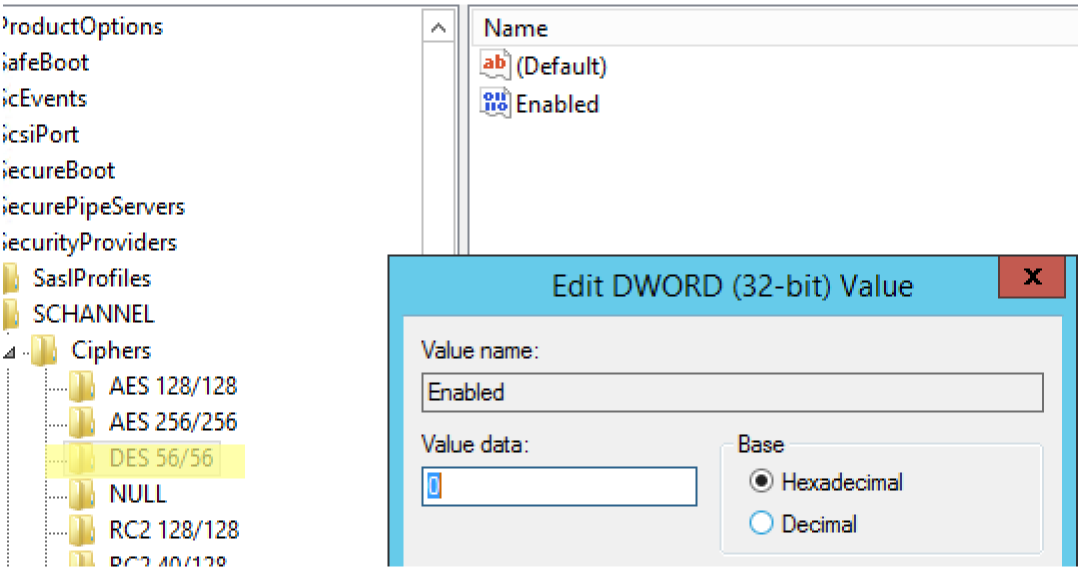
Open: regedit.exe

Navigate to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers

Set 0 to
NULL
DES 56/56
RC2 40/128
RC2 56/128
RC2 128/128
RC4 40/128
RC4 56/128
RC4 64/128
RC4 128/128
Triple DES 168

Take DES 56/56 as example



Edit DWORD (32-bit) Value

Value name: Enabled

Value data: 0

Base

● Hexadecimal

○ Decimal

Navigate to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols

Set key as below

SSL 2.0

Key: Client DWORD: DisabledByDefault (1)

Key: Client DWORD: Enabled (0)

Key: Server DWORD: DisabledByDefault (1)

Key: Server DWORD: Enabled (0)

SSL 3.0

Key: Client DWORD: DisabledByDefault (1)

Key: Client DWORD: Enabled (0)

Key: Server DWORD: DisabledByDefault (1)

Key: Server DWORD: Enabled (0)

TLS 1.0 *

Key: Client DWORD: DisabledByDefault (1)

Key: Client DWORD: Enabled (0)

Key: Server DWORD: DisabledByDefault (1)

Key: Server DWORD: Enabled (0)

TLS 1.1

Key: Client DWORD: DisabledByDefault (1)

Key: Client DWORD: Enabled (0)

Key: Server DWORD: DisabledByDefault (1)

Key: Server DWORD: Enabled (0)

TLS 1.2

Key: Client DWORD: DisabledByDefault (0)

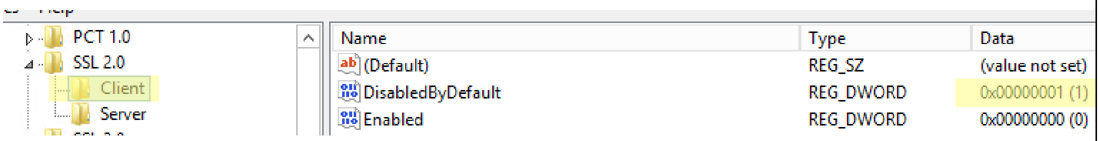
Key: Client DWORD: Enabled (1)

Key: Server DWORD: DisabledByDefault (0)

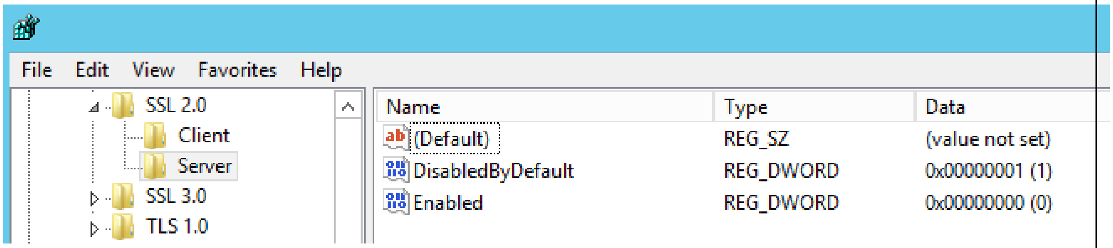
Key: Server DWORD: Enabled (1)

Result is

SSL 2.0

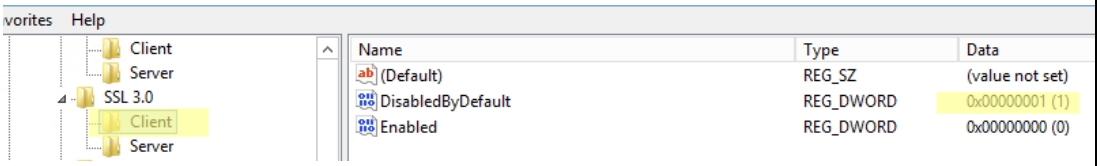


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

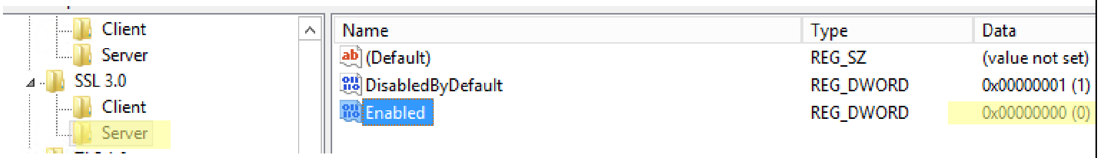


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

SSL 3.0

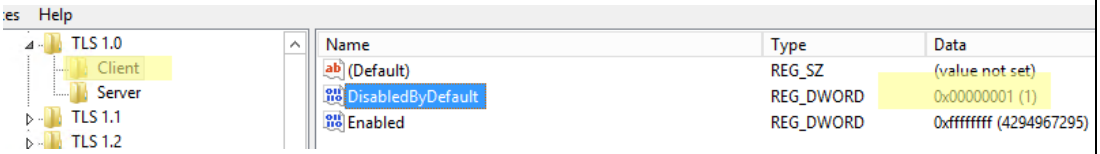


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

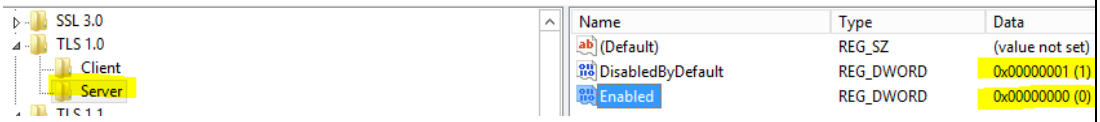


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

TLS 1.0

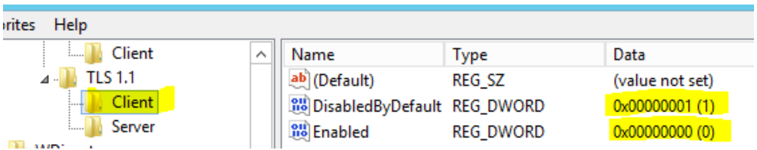


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0xffffffff (4294967295)

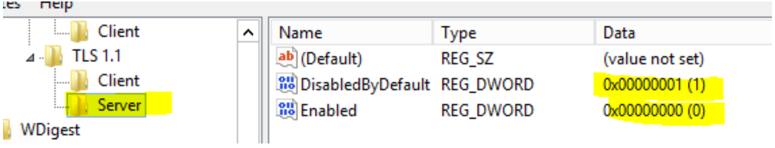


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

TLS1.1

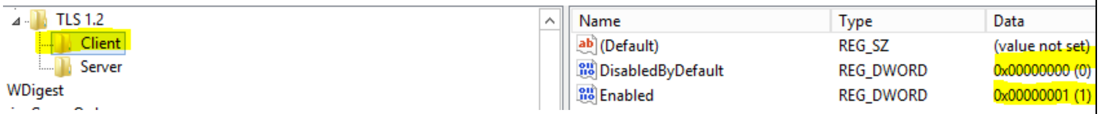


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

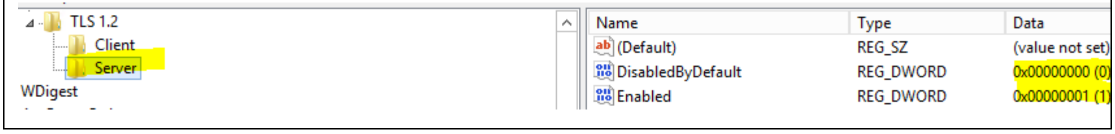


Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000001 (1)
Enabled	REG_DWORD	0x00000000 (0)

TLS1.2



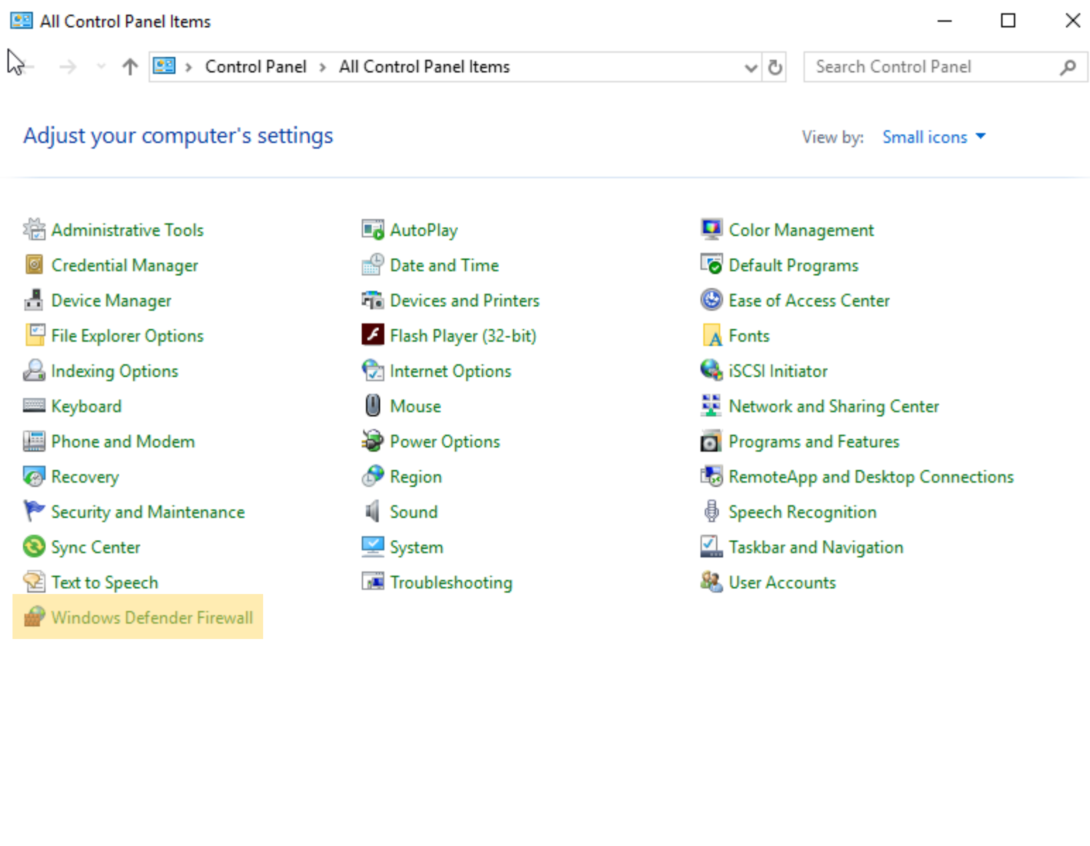
Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

2.5 Firewall

In All Control Panel Items , click Windows Defender Firewall



All Control Panel Items

Control Panel > All Control Panel Items

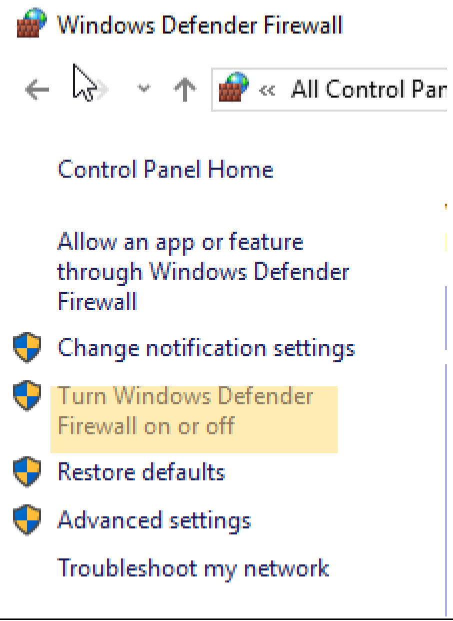
Search Control Panel

Adjust your computer's settings

View by: Small icons

- Administrative Tools
- Credential Manager
- Device Manager
- File Explorer Options
- Indexing Options
- Keyboard
- Phone and Modem
- Recovery
- Security and Maintenance
- Sync Center
- Text to Speech
- Windows Defender Firewall
- AutoPlay
- Date and Time
- Devices and Printers
- Flash Player (32-bit)
- Internet Options
- Mouse
- Power Options
- Region
- Sound
- System
- Troubleshooting
- Color Management
- Default Programs
- Ease of Access Center
- Fonts
- iSCSI Initiator
- Network and Sharing Center
- Programs and Features
- RemoteApp and Desktop Connections
- Speech Recognition
- Taskbar and Navigation
- User Accounts

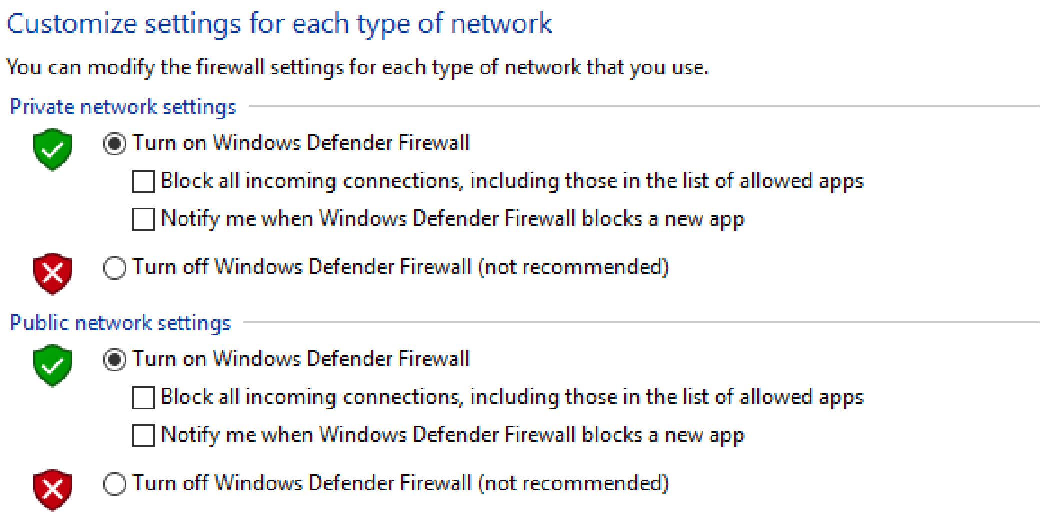
Activate firewall



Windows Defender Firewall

« All Control Par

- Control Panel Home
- Allow an app or feature through Windows Defender Firewall
- Change notification settings
- Turn Windows Defender Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

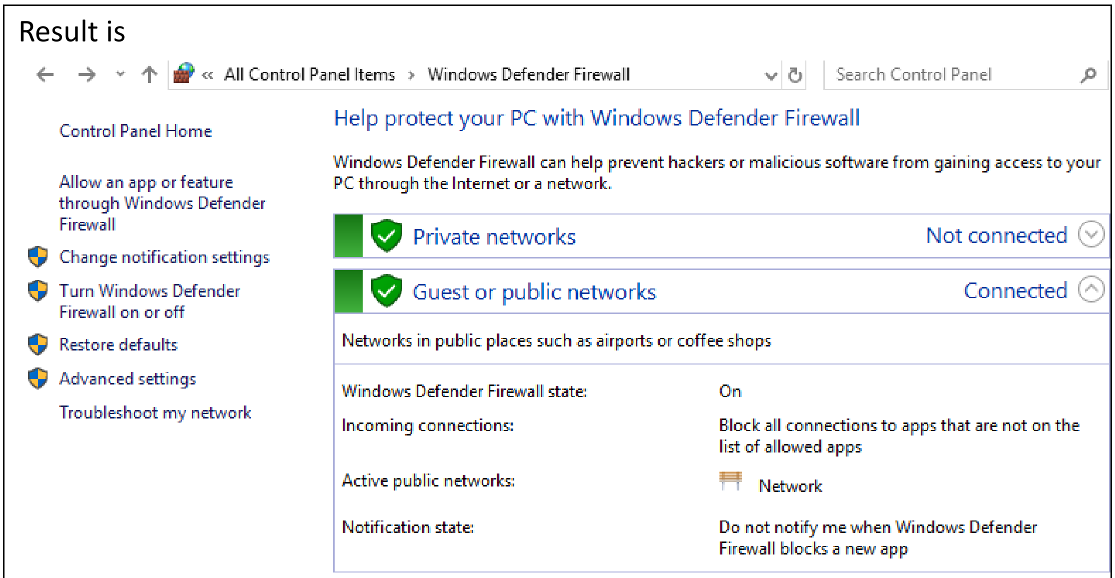
● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Result is



« All Control Panel Items › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

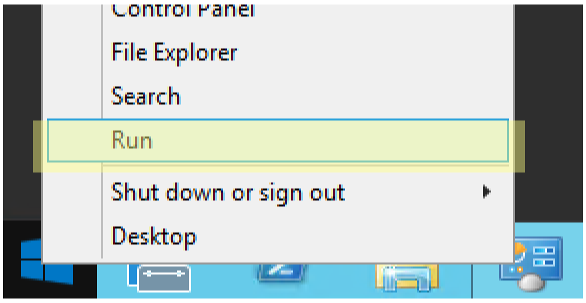
Private networks — Not connected

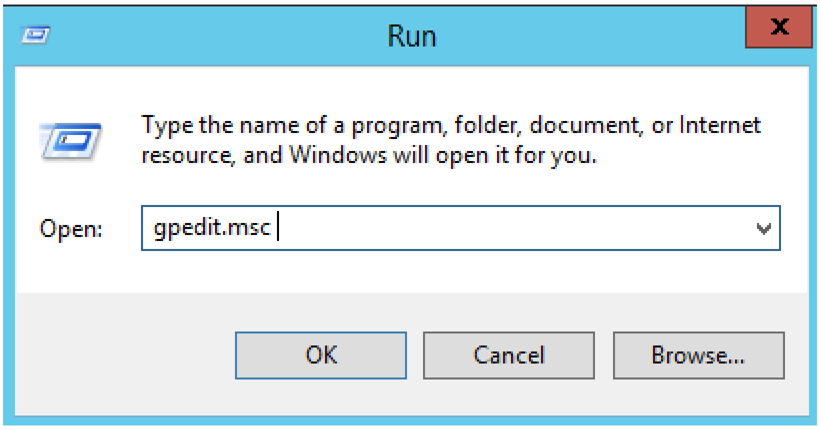
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network
Notification state:	Do not notify me when Windows Defender Firewall blocks a new app

Run gpedit.msc





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

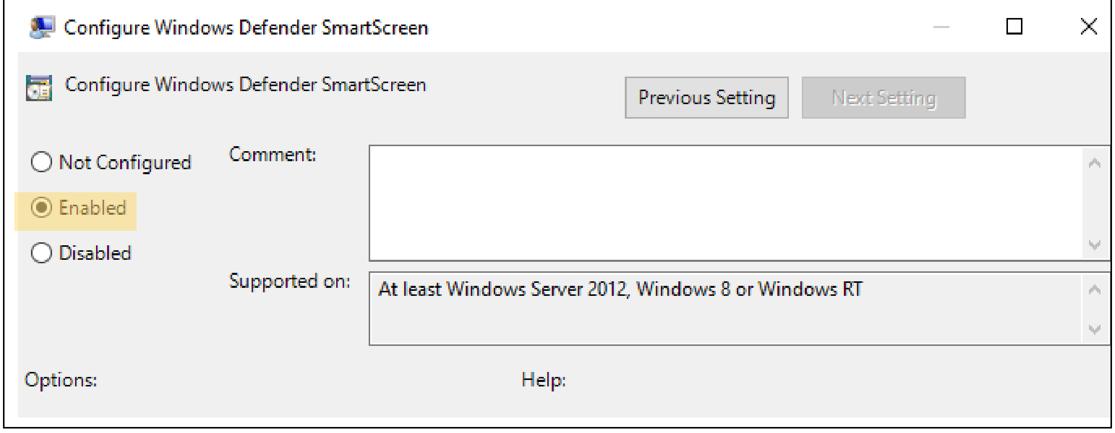
Open: gpedit.msc

Navigate to

Computer Configuration – Administrative Template – Windows Components – Windows Defender SmartScreen – Explorer

Click Configure Windows Defender SmartScreen

Select Enabled



Configure Windows Defender SmartScreen

Configure Windows Defender SmartScreen

○ Not Configured
● Enabled
○ Disabled

Comment:

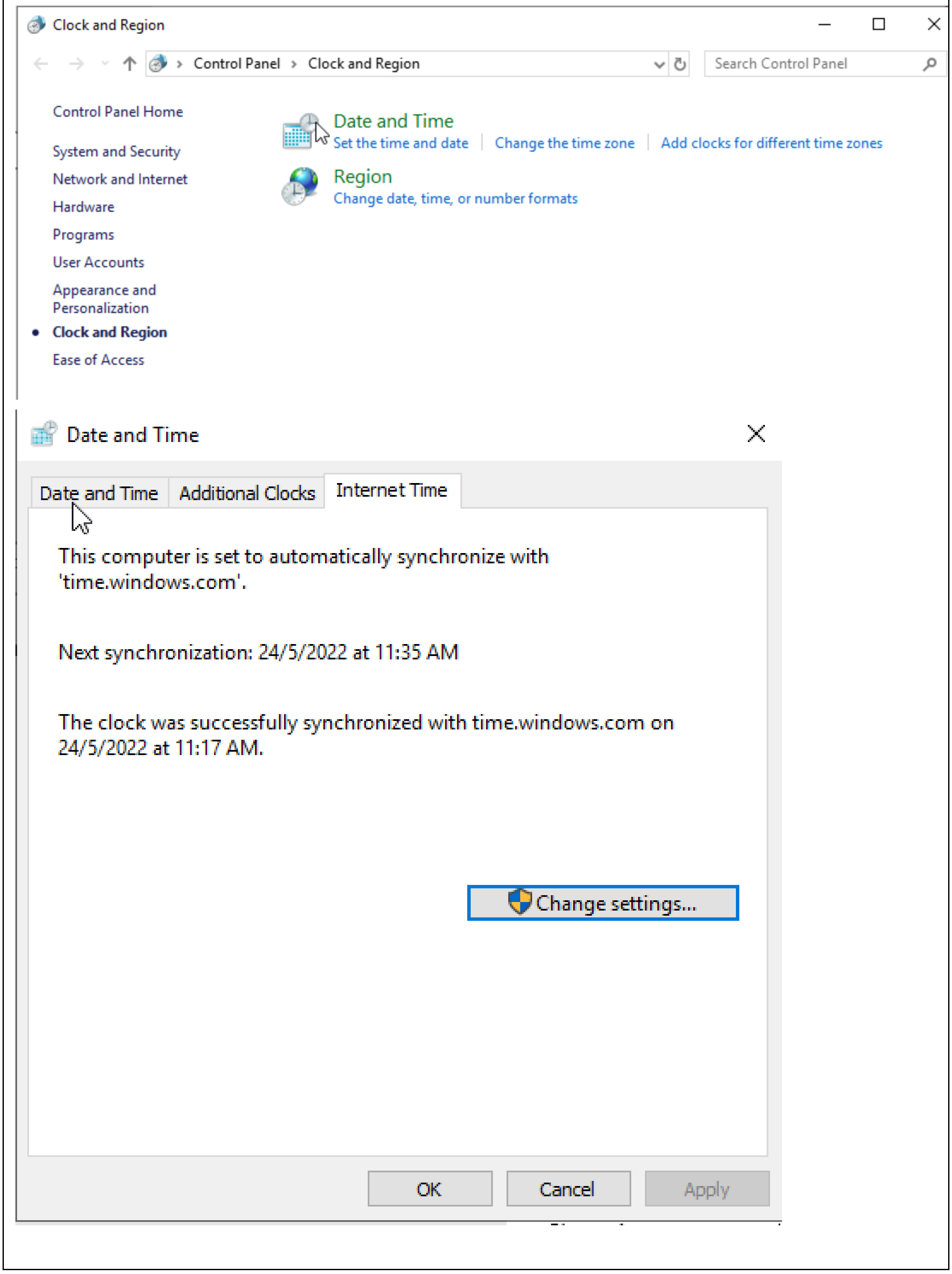
Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Help:

2.6 NTP (Time Synchronization)

Open Control Panel, navigate to Clock and Region, click Date and Time



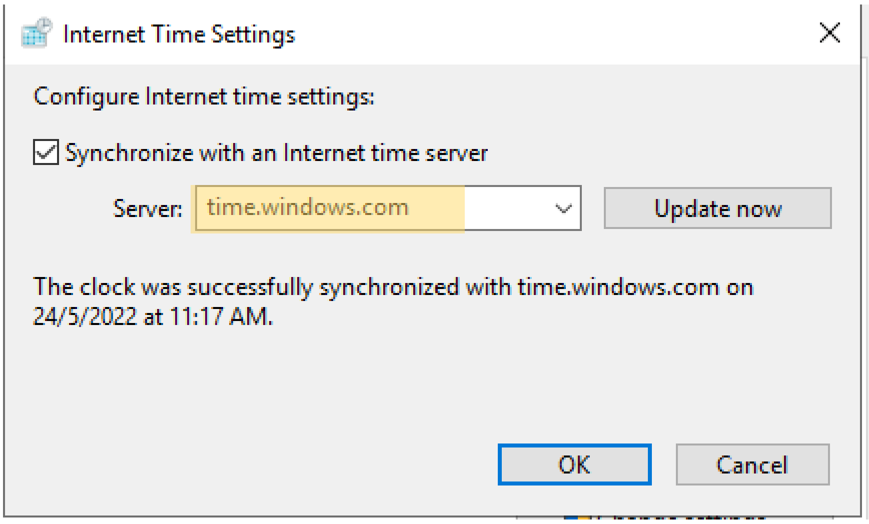
This computer is set to automatically synchronize with 'time.windows.com'.

Next synchronization: 24/5/2022 at 11:35 AM

The clock was successfully synchronized with time.windows.com on 24/5/2022 at 11:17 AM.

Click Change settings

Set your prefered time source, such as your internal domain server or internet time server.



Configure Internet time settings:

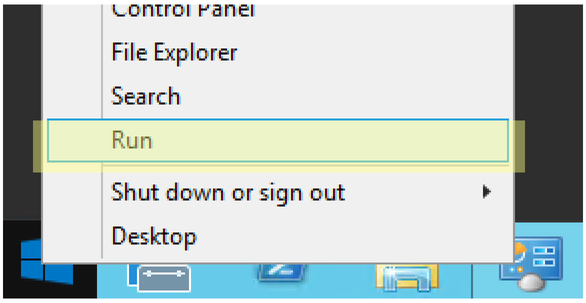
☑ Synchronize with an Internet time server

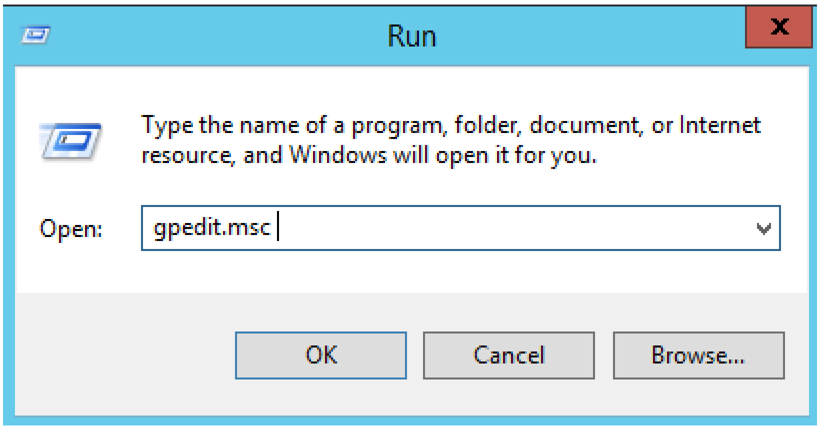
Server: time.windows.com

The clock was successfully synchronized with time.windows.com on 24/5/2022 at 11:17 AM.

2.7 Remote Desktop Configuration

Run gpedit.msc



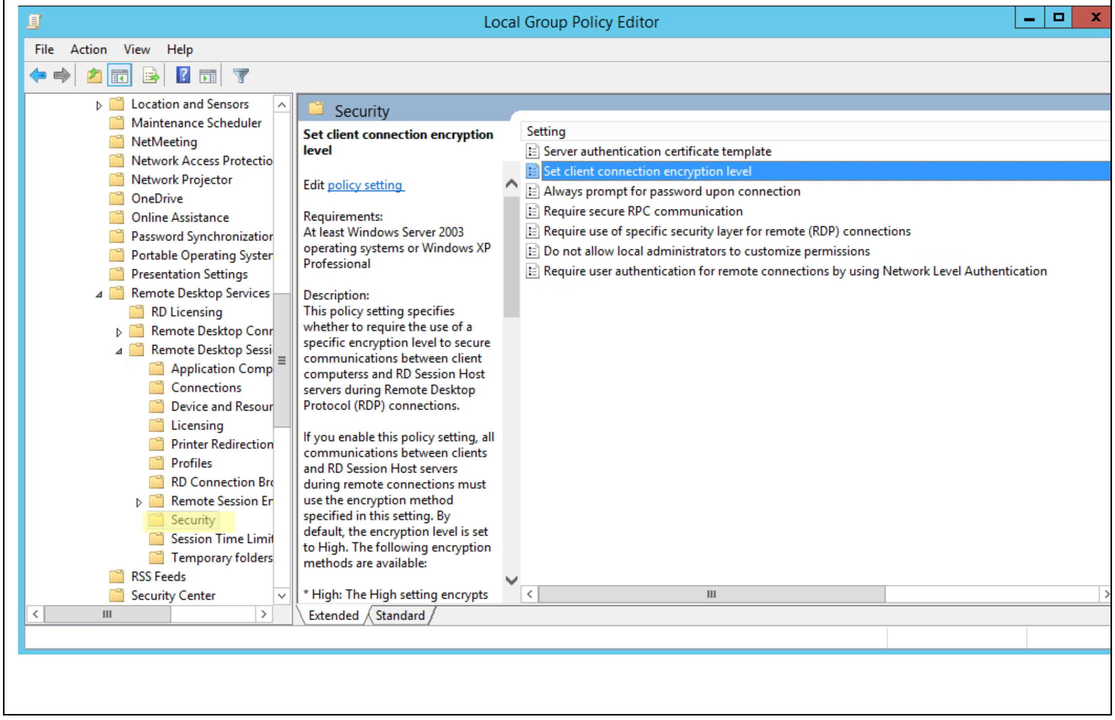


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

Navigate to

Computer Configuration - Administrative Templates - Windows Components - Remote Desktop Services - Remote Desktop Session Host - Security



- Location and Sensors
- Maintenance Scheduler
- NetMeeting
- Network Access Protectio
- Network Projector
- OneDrive
- Online Assistance
- Password Synchronizatior
- Portable Operating Syster
- Presentation Settings
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Conr
  - Remote Desktop Sessi
    - Application Comp
    - Connections
    - Device and Resour
    - Licensing
    - Printer Redirection
    - Profiles
    - RD Connection Br
    - Remote Session Er
    - Security
    - Session Time Limit
    - Temporary folders
- RSS Feeds
- Security Center

Security

Set client connection encryption level

Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

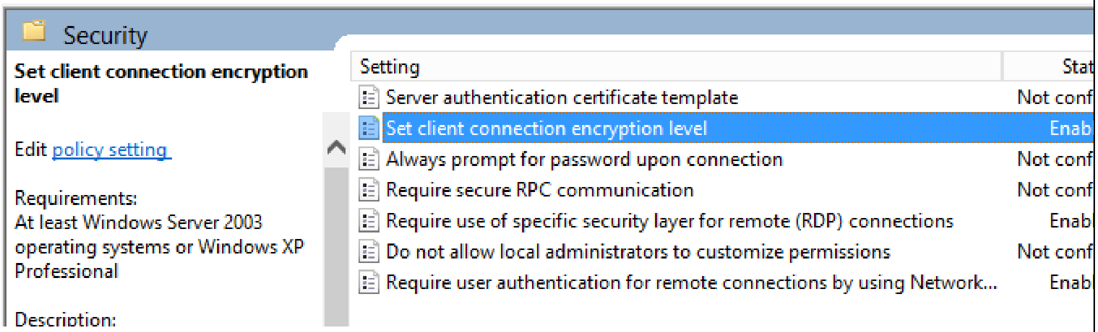
Description:
This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computerss and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the encryption method specified in this setting. By default, the encryption level is set to High. The following encryption methods are available:

* High: The High setting encrypts

Setting
- Server authentication certificate template
- Set client connection encryption level
- Always prompt for password upon connection
- Require secure RPC communication
- Require use of specific security layer for remote (RDP) connections
- Do not allow local administrators to customize permissions
- Require user authentication for remote connections by using Network Level Authentication

Click Set client connection encryption level



Set client connection encryption level

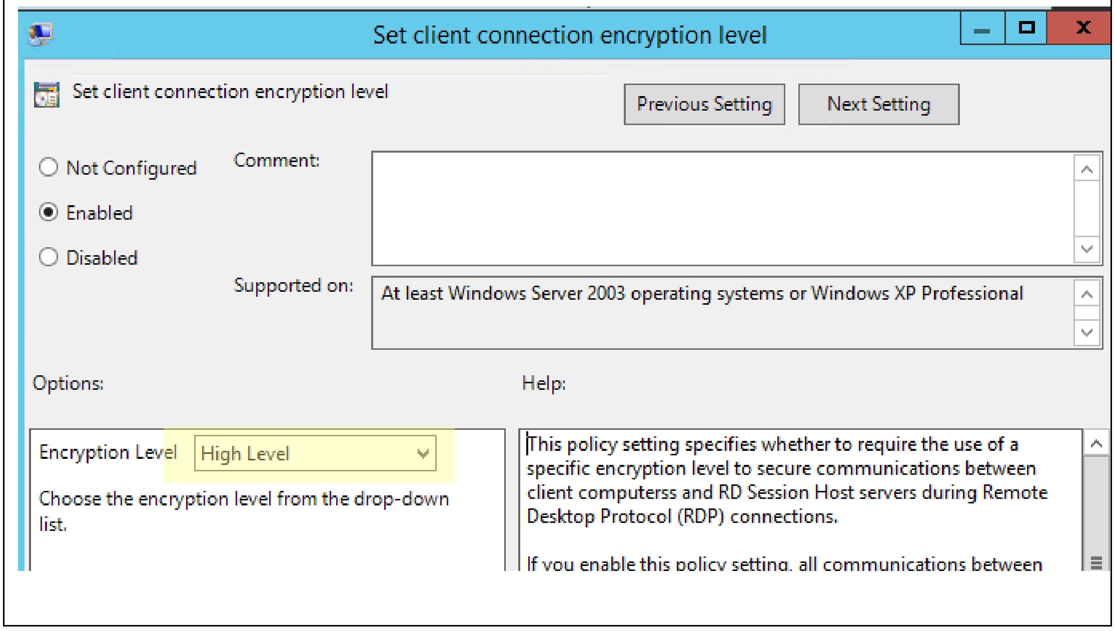
Edit policy setting

Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional

Description:

Setting	Stat
Server authentication certificate template	Not conf
Set client connection encryption level	Enab
Always prompt for password upon connection	Not conf
Require secure RPC communication	Not conf
Require use of specific security layer for remote (RDP) connections	Enab
Do not allow local administrators to customize permissions	Not conf
Require user authentication for remote connections by using Network...	Enab

Select High Level



Set client connection encryption level
Set client connection encryption level
Previous Setting
Next Setting

○ Not Configured

● Enabled

○ Disabled

Comment:

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

Options:

Encryption Level: High Level

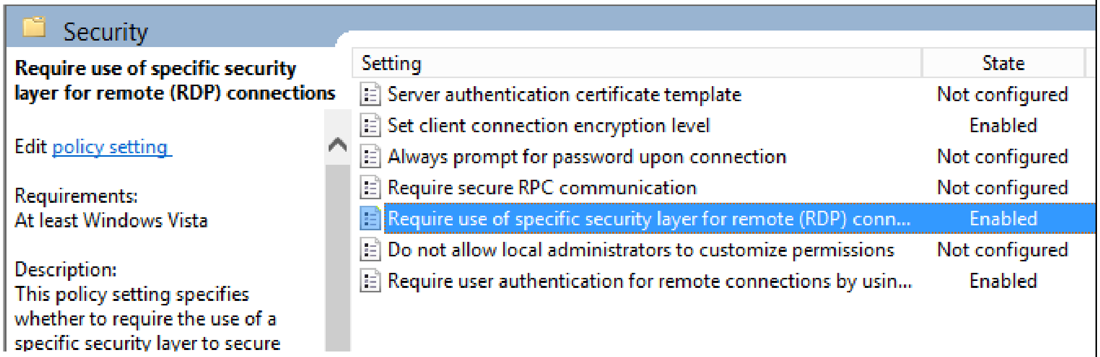
Choose the encryption level from the drop-down list.

Help:

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computerss and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

If you enable this policy setting, all communications between

Click Require use of specific security layer for remote (RDP) connections



Security

Require use of specific security layer for remote (RDP) connections

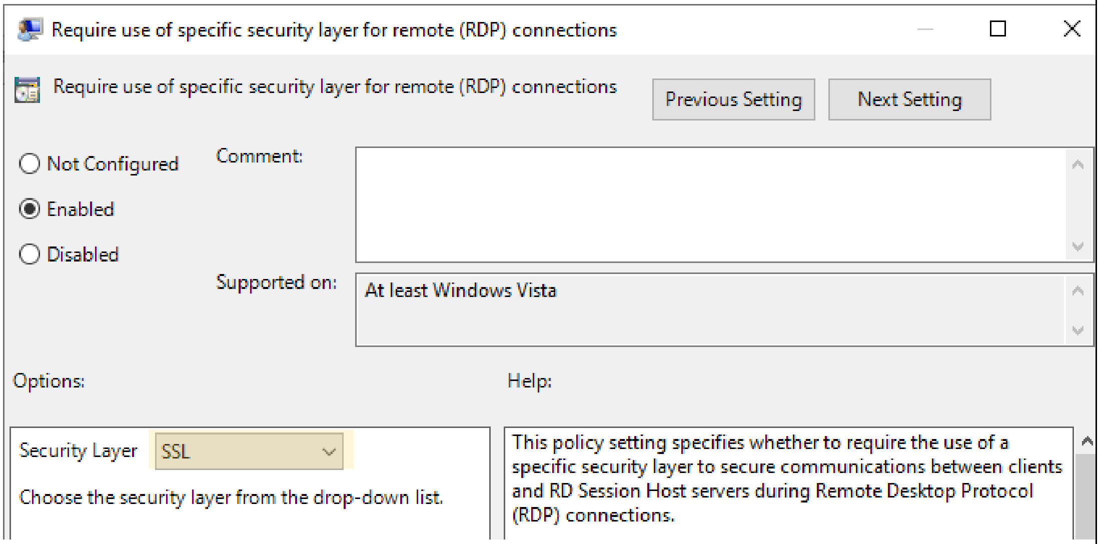
Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting specifies whether to require the use of a specific security layer to secure

Setting	State
Server authentication certificate template	Not configured
Set client connection encryption level	Enabled
Always prompt for password upon connection	Not configured
Require secure RPC communication	Not configured
Require use of specific security layer for remote (RDP) conn...	Enabled
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by usin...	Enabled

Select SSL



Require use of specific security layer for remote (RDP) connections

Require use of specific security layer for remote (RDP) connections

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

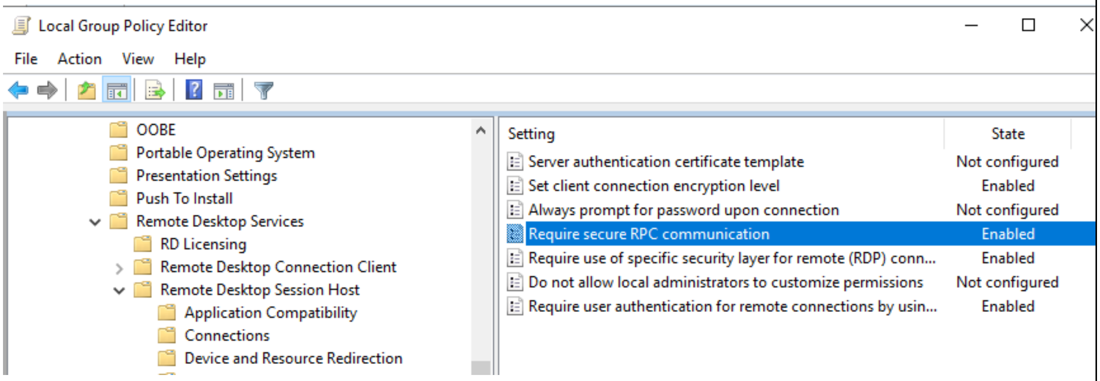
Security Layer: SSL

Choose the security layer from the drop-down list.

Help:

This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.

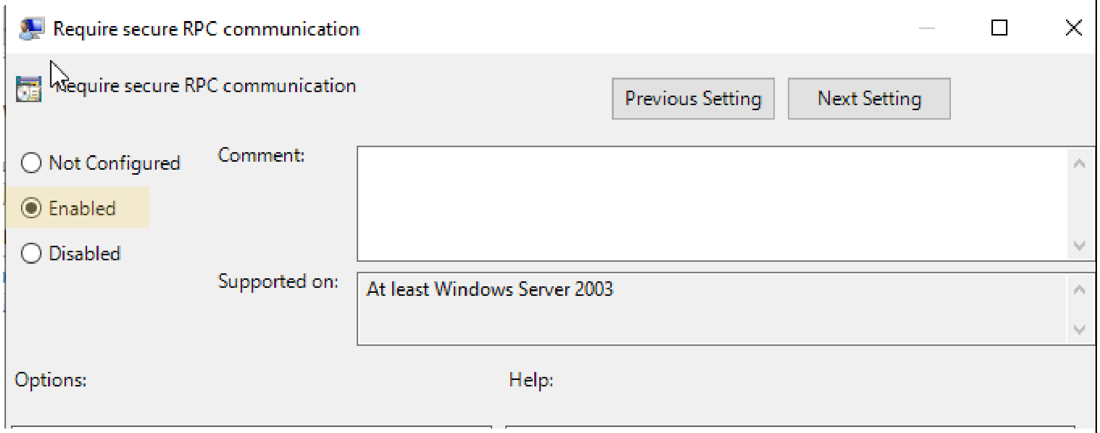
Click Require secure RPC communication



- OOBE
- Portable Operating System
- Presentation Settings
- Push To Install
- Remote Desktop Services
  - RD Licensing
  - Remote Desktop Connection Client
  - Remote Desktop Session Host
    - Application Compatibility
    - Connections
    - Device and Resource Redirection

Setting	State
Server authentication certificate template	Not configured
Set client connection encryption level	Enabled
Always prompt for password upon connection	Not configured
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) conn...	Enabled
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by usin...	Enabled

Select Enabled


Require secure RPC communication
Require secure RPC communication
Previous Setting
Next Setting

○ Not Configured

● Enabled

○ Disabled

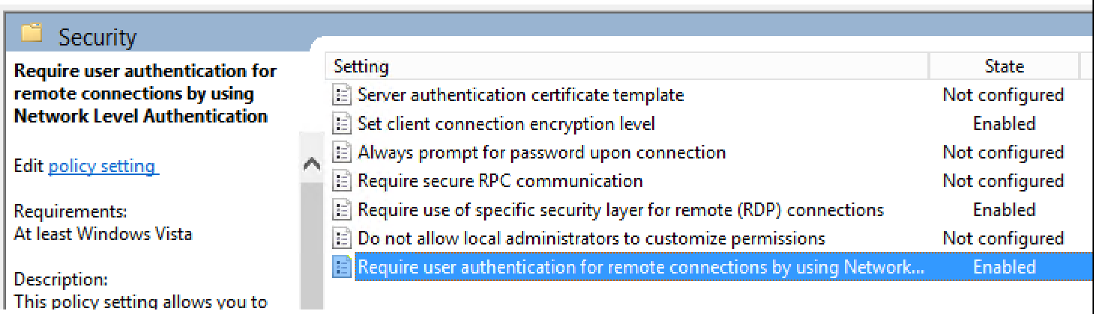
Comment:

Supported on: At least Windows Server 2003

Options:

Help:

Click Require user authentication for remote connections by using Network Level Authentication



Security

Require user authentication for remote connections by using Network Level Authentication

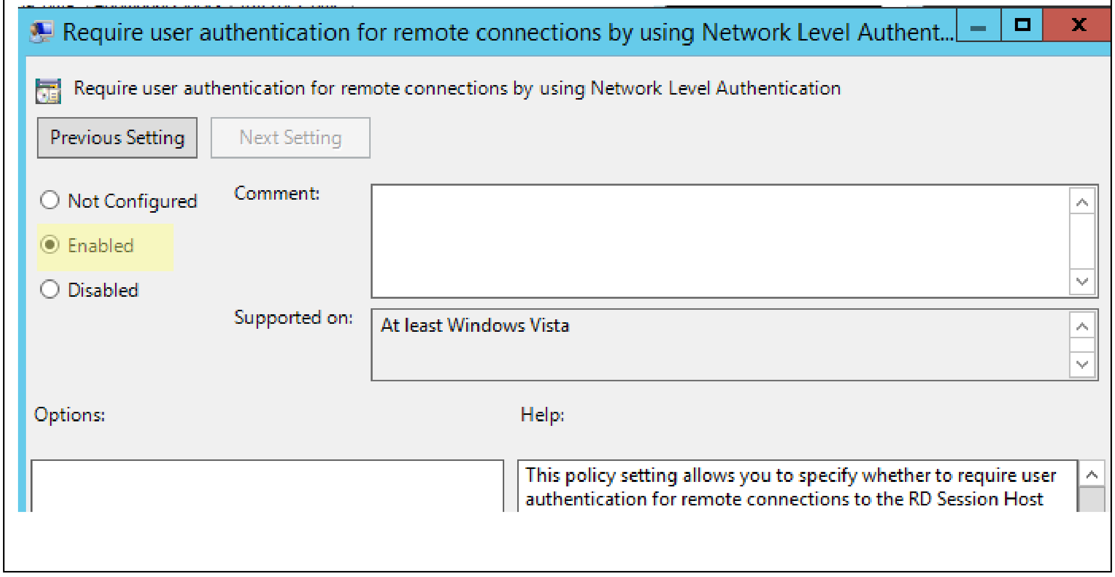
Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting allows you to

Setting	State
Server authentication certificate template	Not configured
Set client connection encryption level	Enabled
Always prompt for password upon connection	Not configured
Require secure RPC communication	Not configured
Require use of specific security layer for remote (RDP) connections	Enabled
Do not allow local administrators to customize permissions	Not configured
Require user authentication for remote connections by using Network...	Enabled

Select Enabled



Require user authentication for remote connections by using Network Level Authent...

Require user authentication for remote connections by using Network Level Authentication

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows Vista

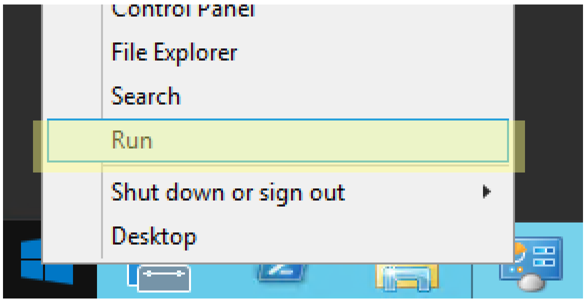
Options:

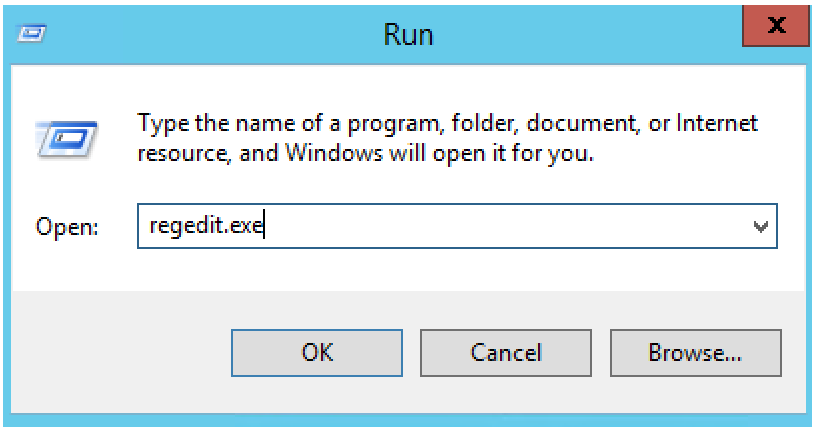
Help:

This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host

2.8 Unquoted Service Path

Run regedit.exe (registry editor)



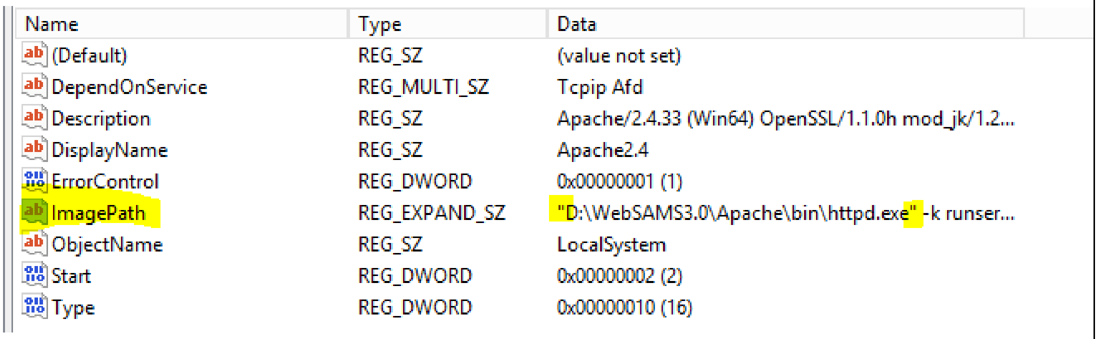


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit.exe

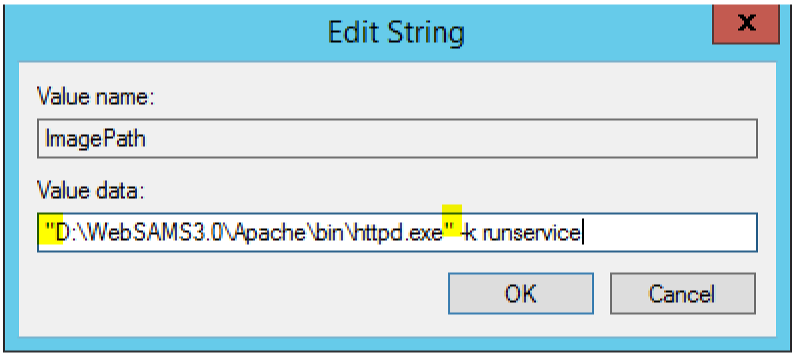
Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

For each key (service), check if the path to the executable file in the ImagePath is double quoted.



Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab DependOnService	REG_MULTI_SZ	Tcpip Afd
ab Description	REG_SZ	Apache/2.4.33 (Win64) OpenSSL/1.1.0h mod_jk/1.2...
ab DisplayName	REG_SZ	Apache2.4
ErrorControl	REG_DWORD	0x00000001 (1)
ab ImagePath	REG_EXPAND_SZ	"D:\WebSAMS3.0\Apache\bin\httpd.exe" -k runser...
ab ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

If there is any service executable not double quoted, double click on ImagePath and edit the value data to double quote it.

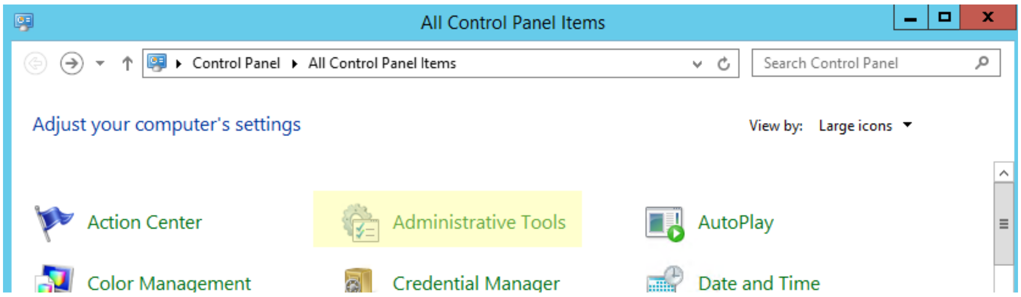


Value name: ImagePath

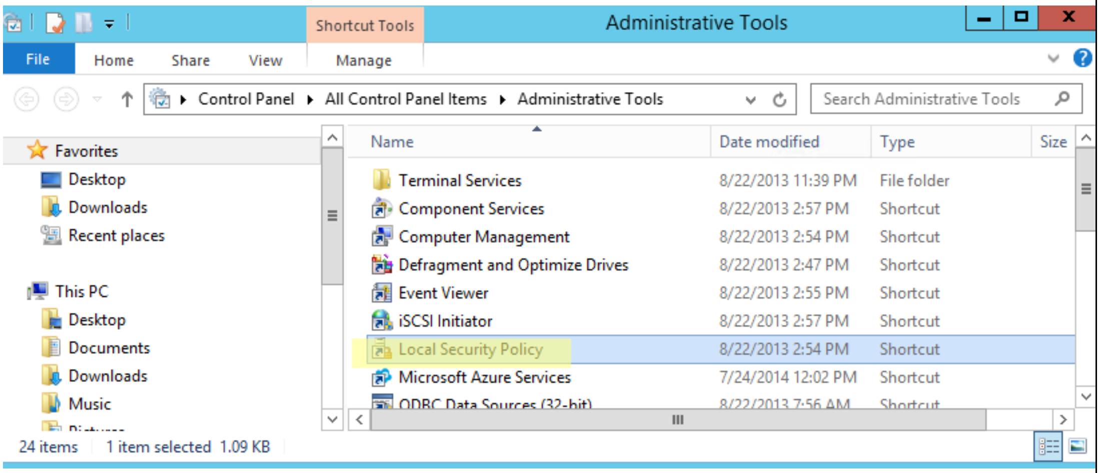
Value data: "D:\WebSAMS3.0\Apache\bin\httpd.exe" -k runservice

2.9 Event Log Setting

In All Control Panel Items , click Administrative Tools



Click Local Security Policy



Name	Date modified	Type	Size
Terminal Services	8/22/2013 11:39 PM	File folder	
Component Services	8/22/2013 2:57 PM	Shortcut	
Computer Management	8/22/2013 2:54 PM	Shortcut	
Defragment and Optimize Drives	8/22/2013 2:47 PM	Shortcut	
Event Viewer	8/22/2013 2:55 PM	Shortcut	
iSCSI Initiator	8/22/2013 2:57 PM	Shortcut	
Local Security Policy	8/22/2013 2:54 PM	Shortcut	
Microsoft Azure Services	7/24/2014 12:02 PM	Shortcut	
ODBC Data Sources (32-bit)	8/22/2013 7:56 AM	Shortcut	

Navigate to

Security Settings – Local Policies – Audit Policy

Check both “Success” & “Failure” options :

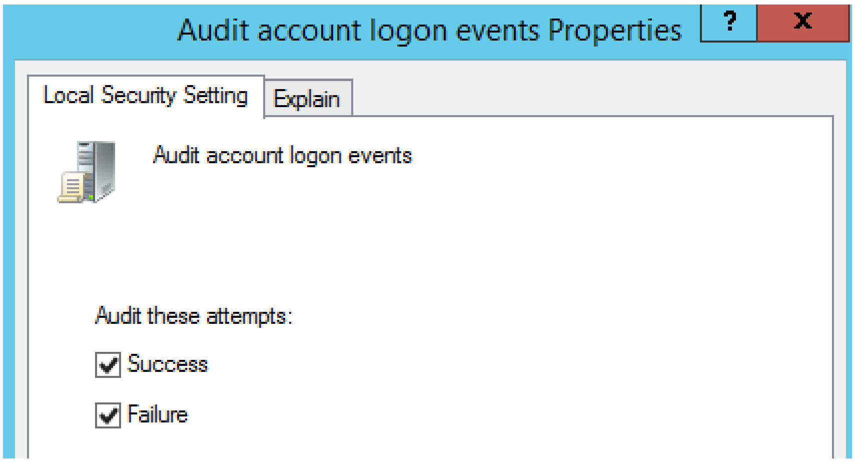
(1) Audit account logon events
(2) Audit account management
(3) Audit directory service access
(4) Audit logon events
(5) Audit object access
(6) Audit policy change
(7) Audit system events

Check “Failure” option for :

(1) Audit privilege use

Uncheck both “Success” & “Failure” options, which means “No auditing” option for :

(1) Audit process tracking



Audit account logon events Properties

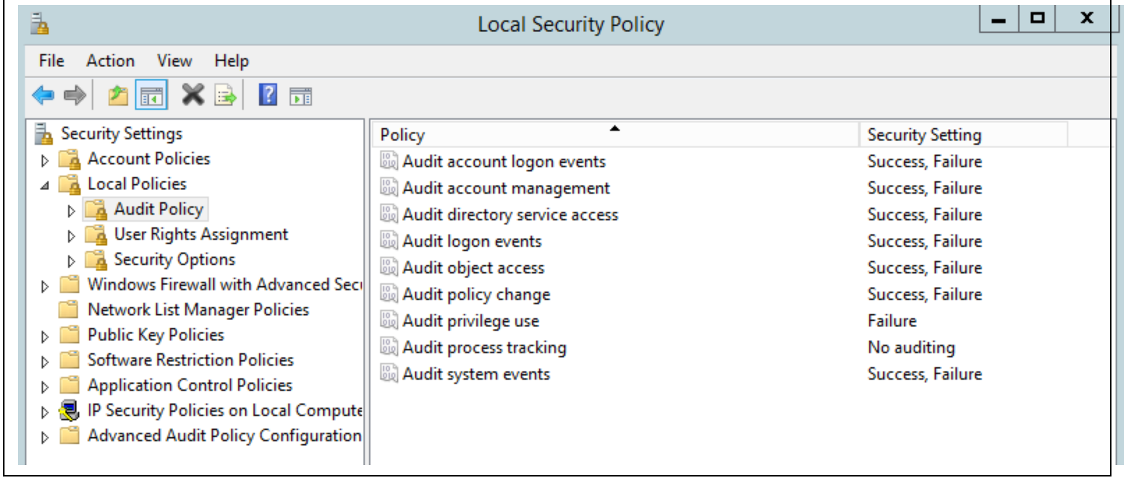
Audit account logon events

Audit these attempts:

☑ Success

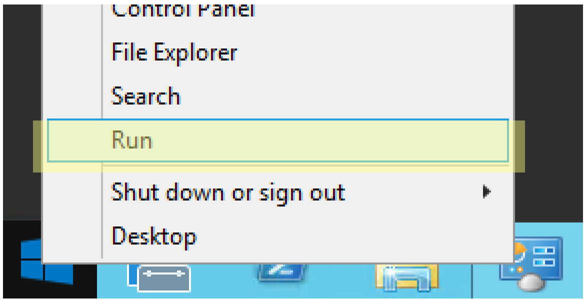
☑ Failure

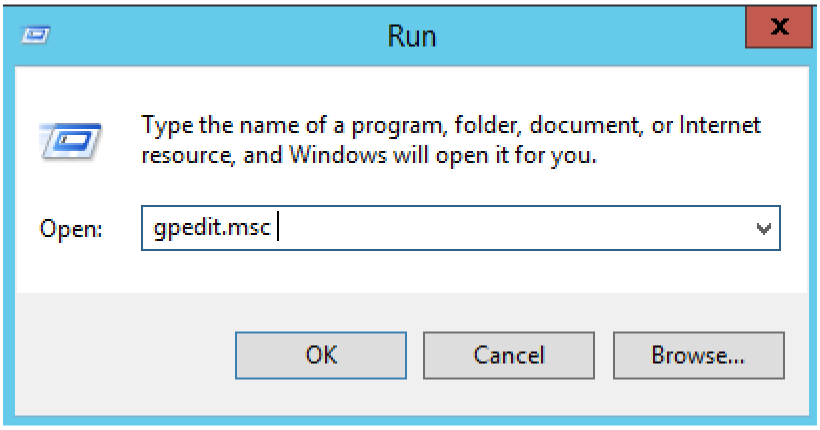
Result is


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Run gpedit.msc





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

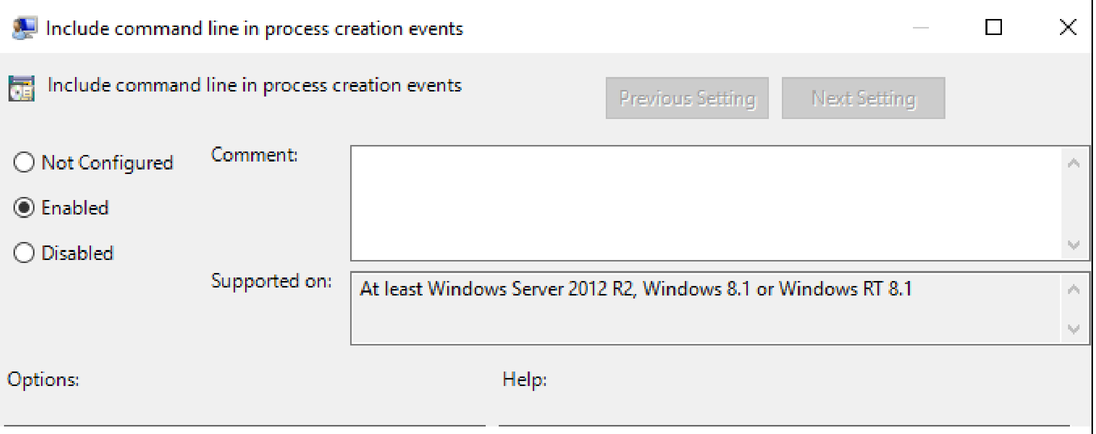
Open: gpedit.msc

Navigate to

Computer Configuration – Administrative Templates – System – Audit Process Creation

Click Include command line in process creation events

Select Enabled



Include command line in process creation events

○ Not Configured
● Enabled
○ Disabled

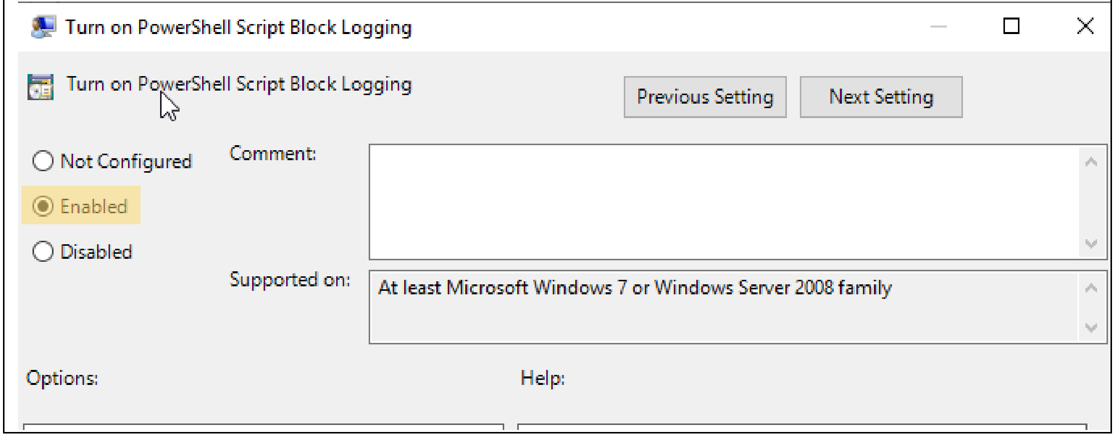
Comment:

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

Navigate to
Computer Configuration – Administrative Templates – Windows Components – Windows PowerShell

Click Turn on PowerShell Script Block Logging

Select Enabled



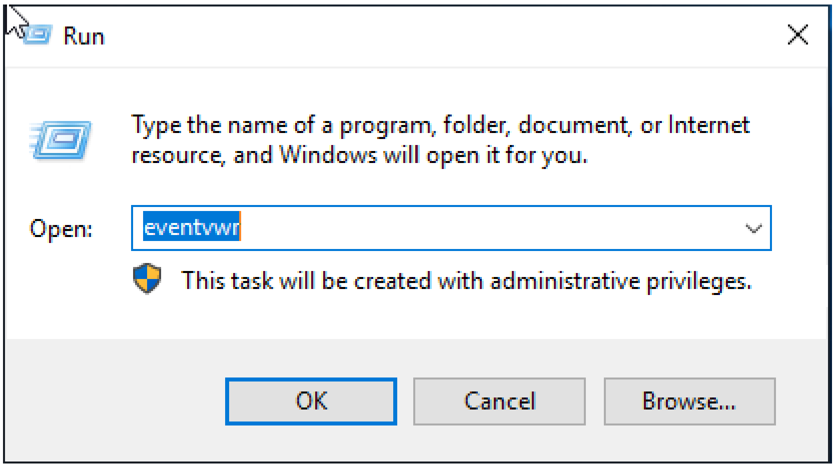
Turn on PowerShell Script Block Logging

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Run eventvwr

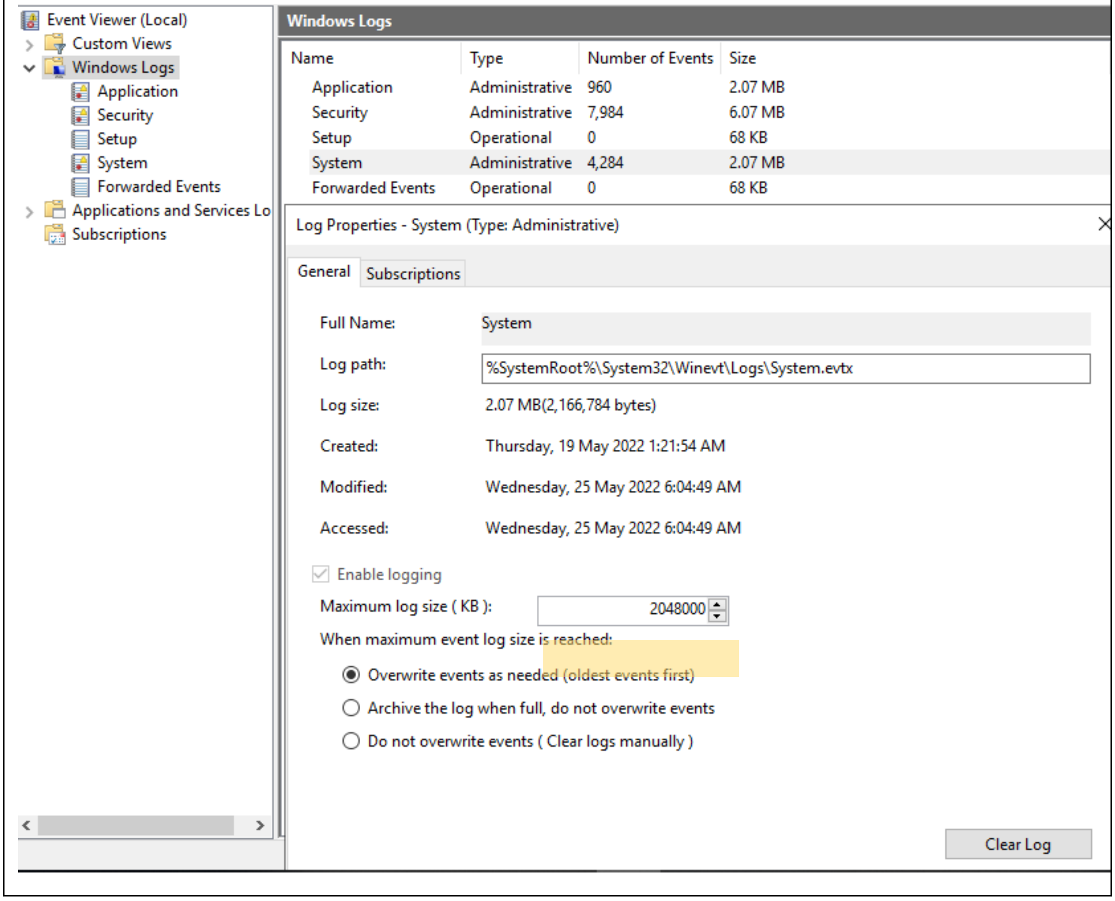


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: eventvwr

This task will be created with administrative privileges.

Go to Event Viewer(Local) – Windows Logs, right click System and selectProperty, set Maximum log size, such as 2GB for System log as below. Apply the same setting for all components under Windows Logs.



Name	Type	Number of Events	Size
Application	Administrative	960	2.07 MB
Security	Administrative	7,984	6.07 MB
Setup	Operational	0	68 KB
System	Administrative	4,284	2.07 MB
Forwarded Events	Operational	0	68 KB

Log Properties - System (Type: Administrative)

Full Name: System

Log path: %SystemRoot%\System32\Winevt\Logs\System.evtx

Log size: 2.07 MB(2,166,784 bytes)

Created: Thursday, 19 May 2022 1:21:54 AM

Modified: Wednesday, 25 May 2022 6:04:49 AM

Accessed: Wednesday, 25 May 2022 6:04:49 AM

☑ Enable logging

Maximum log size (KB): 2048000

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)