MINISTRY OF ICT
Smart Thailand

EGA

e-Government Agency

Electronic Government Agency (Public Organization)
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

การปิดจุดอ่อนวินโดวส์

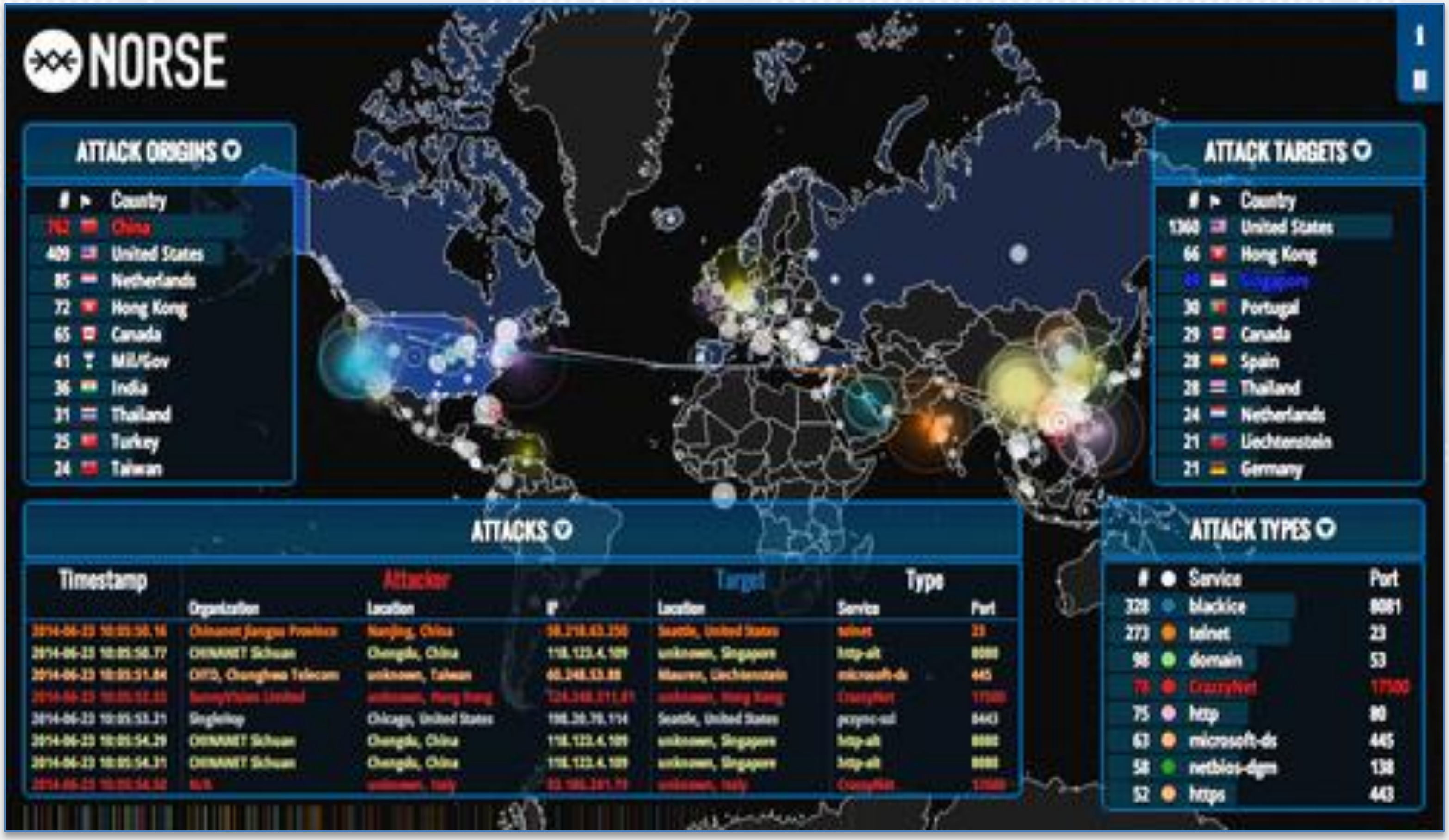
(Windows Hardening)

วัตถุประสงค์การปิดจุดอ่อน

(Harden Objectives)

เพื่อเป็นแนวทางในการกำหนดค่าความปลอดภัยให้กับระบบที่กำลังจะติดตั้งใช้งานจริง หรือการปรับปรุงแก้ไขเครื่องให้บริการที่เกิดมีจุดอ่อนให้มีการป้องกันที่เข้มแข็งขึ้น

ทำไมต้องปิดช่องโหว่



ATTACK ORIGINS

#	▶	Country
762		China
409		United States
85		Netherlands
72		Hong Kong
65		Canada
41		Mil/Gov
36		India
31		Thailand
25		Turkey
24		Taiwan

ATTACK TARGETS

#	▶	Country
1360		United States
66		Hong Kong
[illegible]		Singapore
30		Portugal
29		Canada
28		Spain
28		Thailand
24		Netherlands
21		Liechtenstein
21		Germany

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-23 10:05:50.16	Chinanet Jiangsu Province	Nanjing, China	58.218.63.250	Seattle, United States	telnet	23
2014-06-23 10:05:50.77	CHINANET Sichuan	Chengdu, China	118.123.4.109	unknown, Singapore	http-alt	8080
2014-06-23 10:05:51.84	CHTD, Chunghwa Telecom	unknown, Taiwan	60.248.53.88	Mauren, Liechtenstein	microsoft-ds	445
2014-06-23 10:05:52.32	[illegible]	unknown, Hong Kong	124.248.211.81	unknown, Hong Kong	CrazyNet	17500
2014-06-23 10:05:53.21	SingleHop	Chicago, United States	198.20.70.114	Seattle, United States	pcsync-ssl	8443
2014-06-23 10:05:54.29	CHINANET Sichuan	Chengdu, China	118.123.4.109	unknown, Singapore	http-alt	8080
2014-06-23 10:05:54.31	CHINANET Sichuan	Chengdu, China	118.123.4.109	unknown, Singapore	http-alt	8080
2014-06-23 10:05:54.52	N/A	unknown, Italy	[illegible]	unknown, Italy	CrazyNet	17500

ATTACK TYPES

#	●	Service	Port
328	●	blackice	8081
273	●	telnet	23
98	●	domain	53
78	●	CrazyNet	17500
75	●	http	80
63	●	microsoft-ds	445
58	●	netbios-dgm	138
52	●	https	443

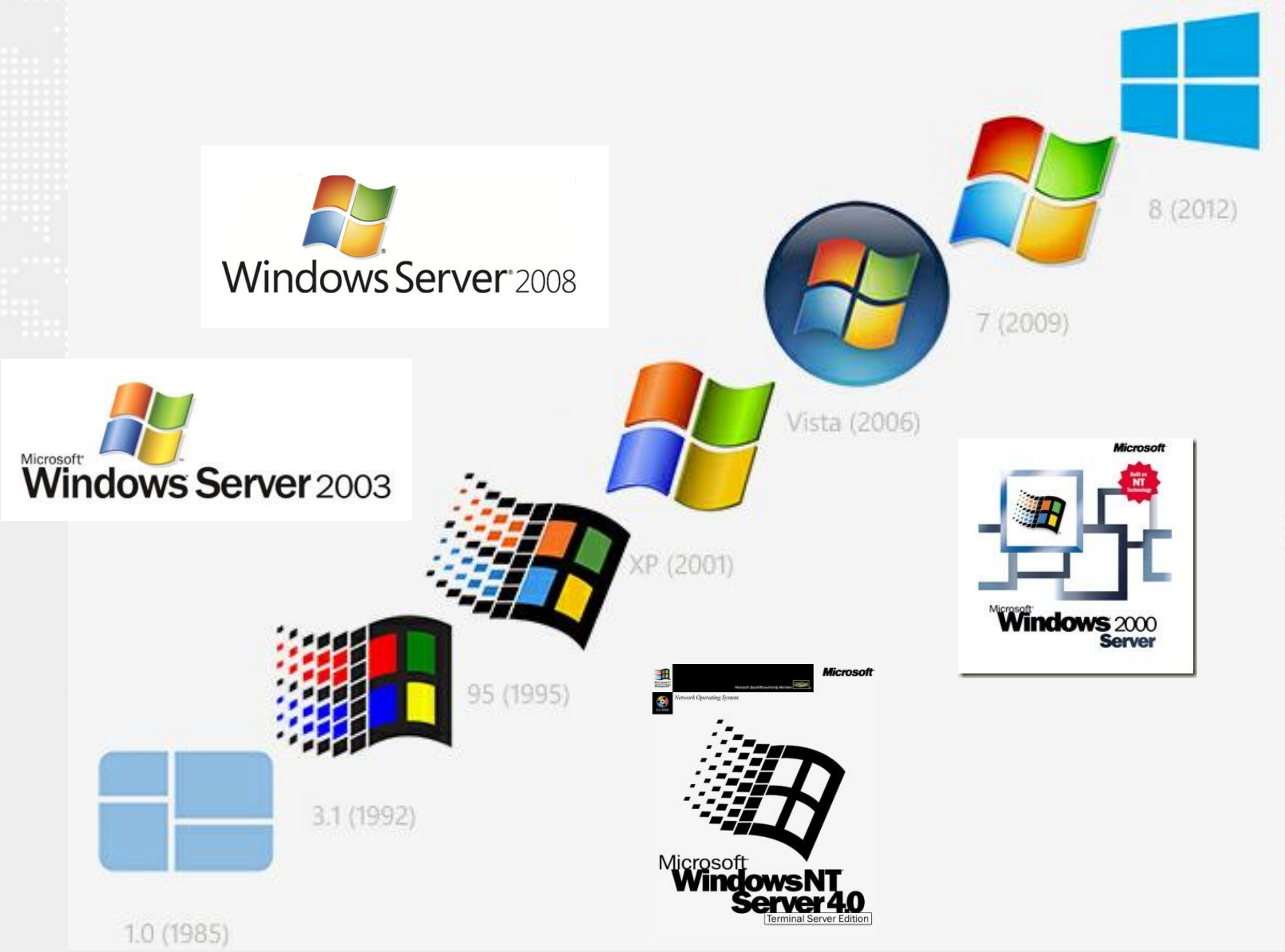
Hardening

- Systems (MS Windows, Linux, Network Devices)
- Application (Mysql, SQL Server, Web Application …)

Microsoft Windows Server 2012 Hardening

- ***Account Policies***
- ***Audit Policy***
- ***Security Options***
- ***Windows Components***
- ***Web Server***
- ***Microsoft Baseline Security Analyzer***

MS Windows Server



Microsoft Corporation

Microsoft Windows

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The National Institute of Standards and Technology (NIST)

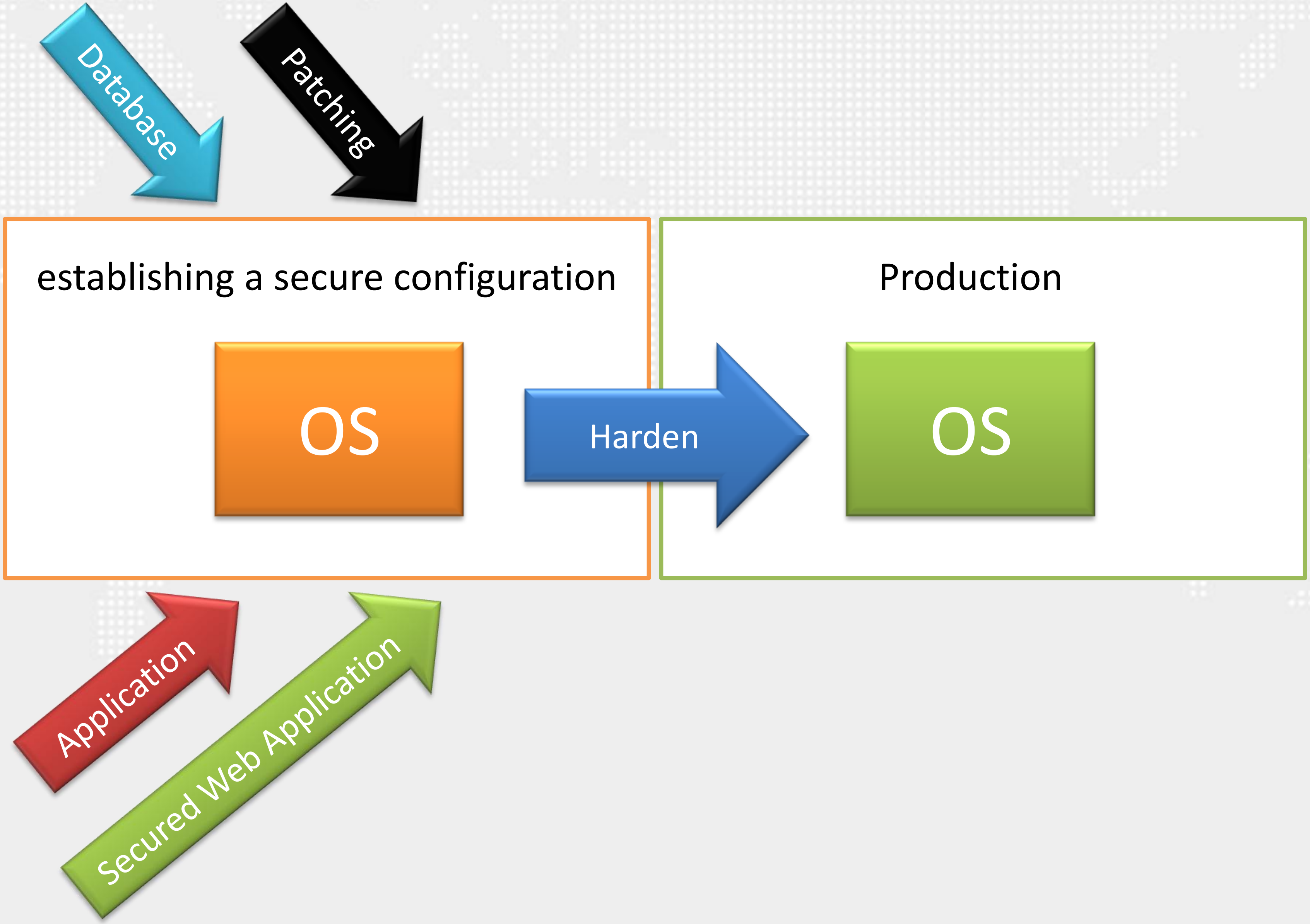
Center for Internet Security (CIS)

Center for Internet Security

http://www.cisecurity.org/

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



Database

Patching

establishing a secure configuration

OS

Harden

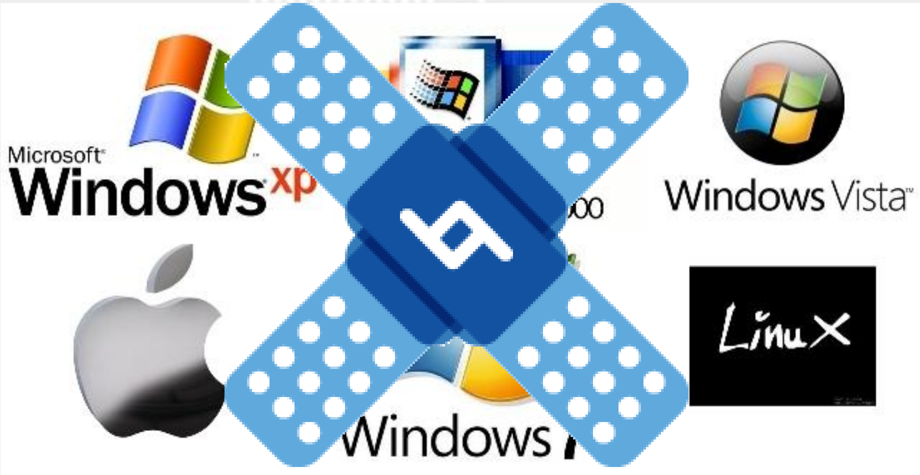
Production

OS

Application

Secured Web Application

Microsoft
Windows XP
NEW
Windows Vista
Linux
Windows 7


Microsoft
Windows XP
Windows Vista
Linux
Windows

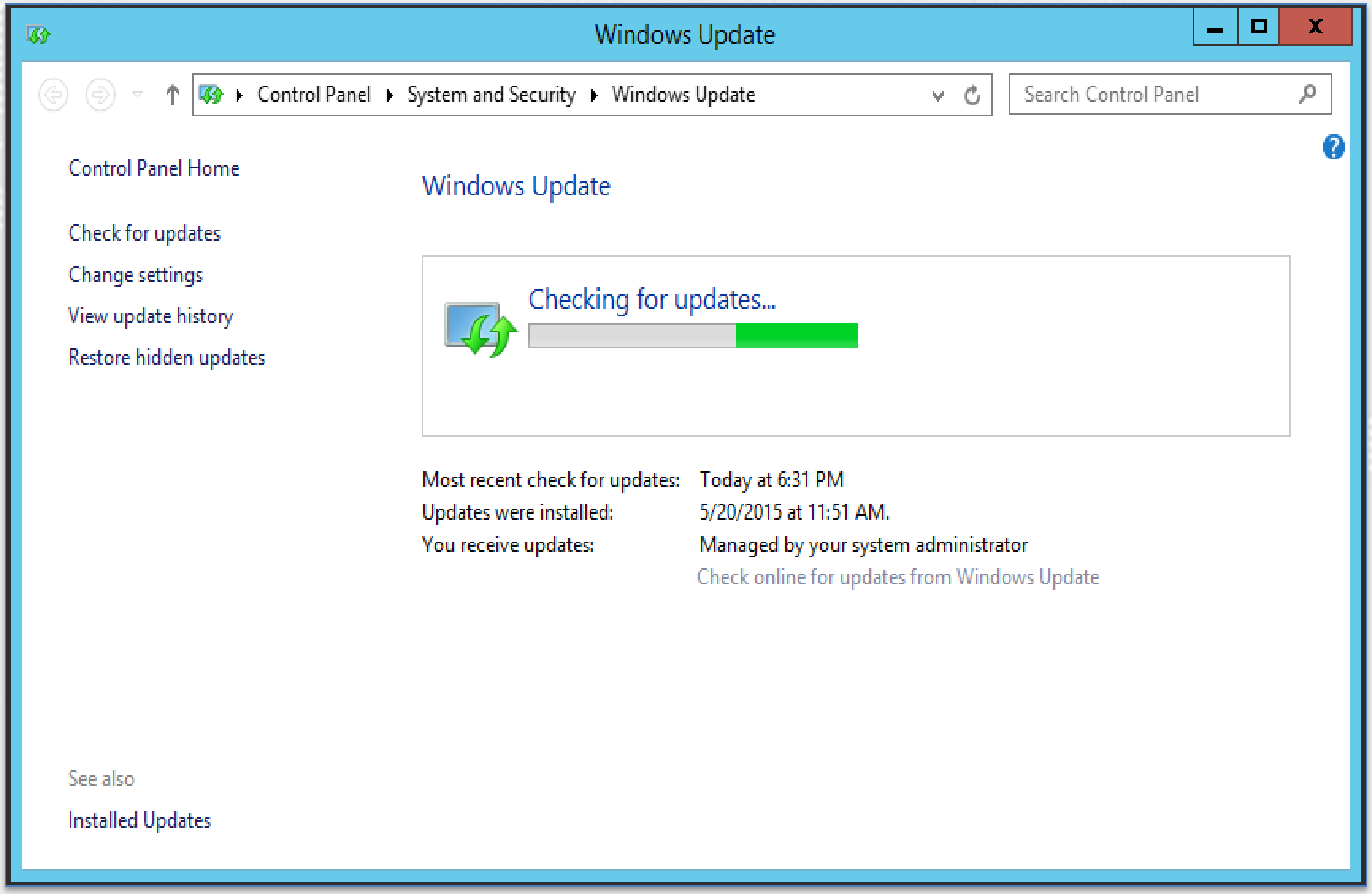
SNMP Community name

Username password

Computer name

Default

Windows Update

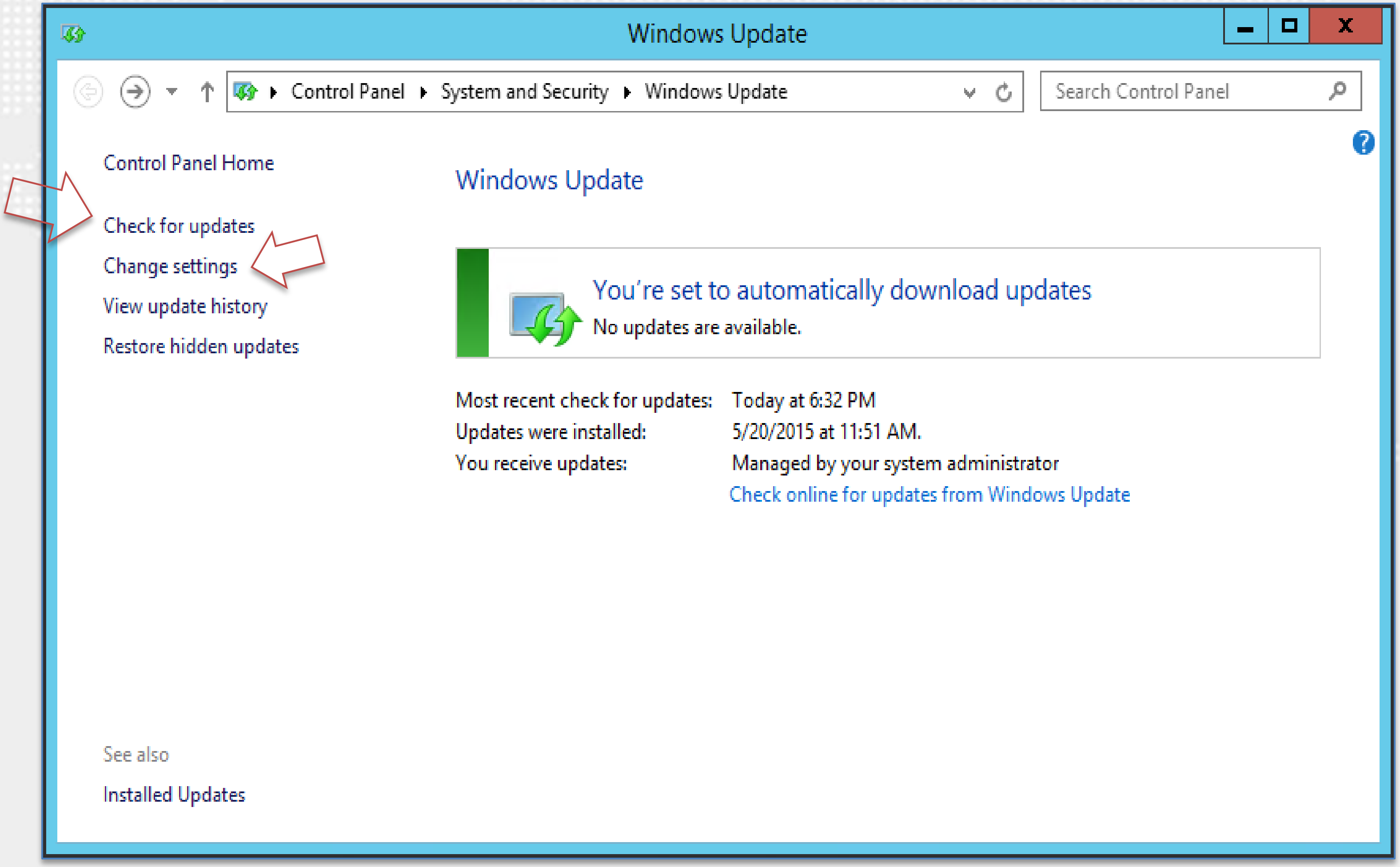


Windows Update

Checking for updates...

Most recent check for updates:	Today at 6:31 PM
Updates were installed:	5/20/2015 at 11:51 AM.
You receive updates:	Managed by your system administrator
	Check online for updates from Windows Update

Windows Update



Windows Update

Control Panel Home

Check for updates

Change settings

View update history

Restore hidden updates

Windows Update

You're set to automatically download updates

No updates are available.

Most recent check for updates: Today at 6:32 PM

Updates were installed: 5/20/2015 at 11:51 AM.

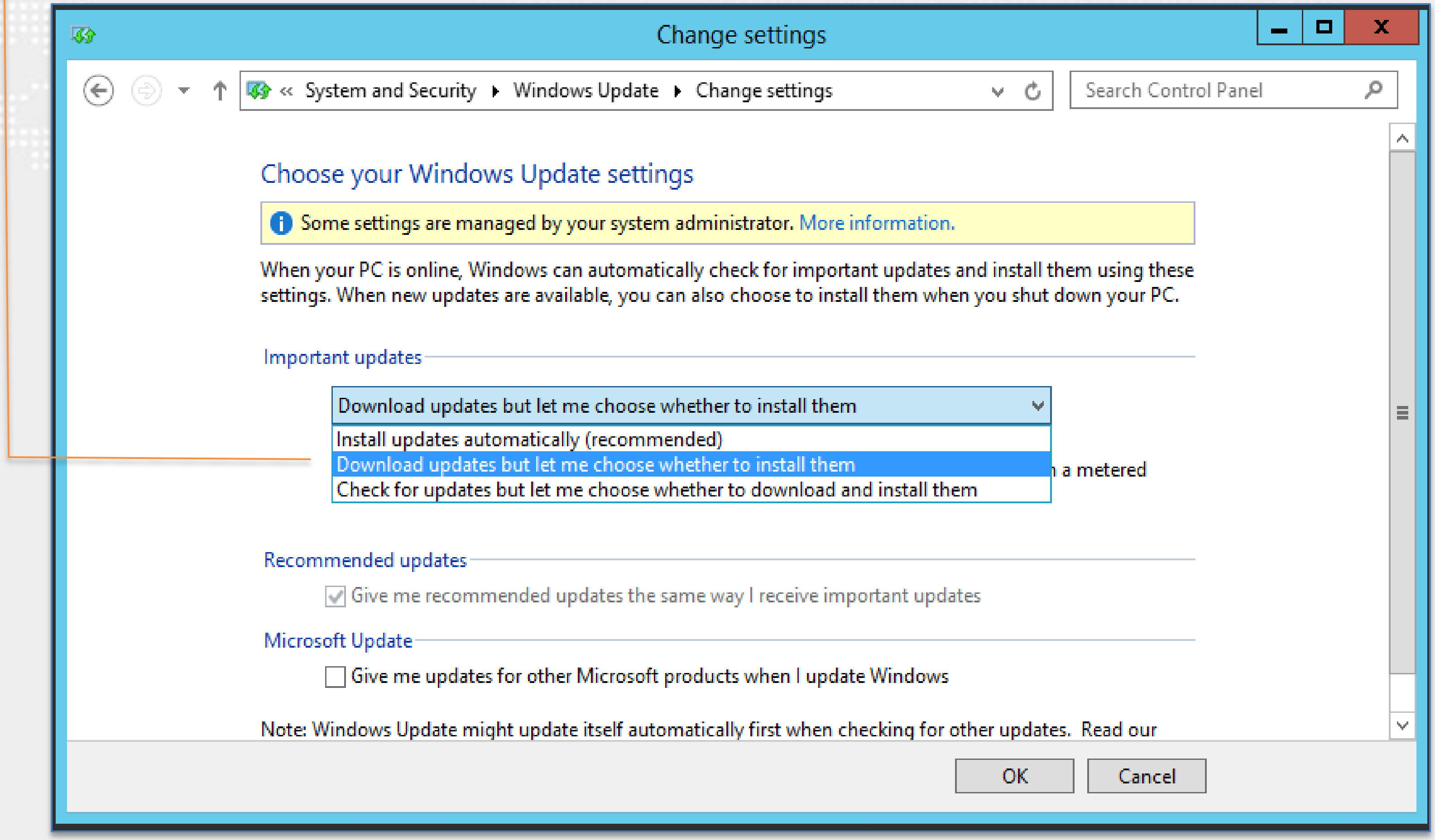
You receive updates: Managed by your system administrator

Check online for updates from Windows Update

See also

Installed Updates

Download updates but let me choose whether to install them



Change settings

System and Security ▸ Windows Update ▸ Change settings

Search Control Panel

Choose your Windows Update settings

Some settings are managed by your system administrator. More information.

When your PC is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also choose to install them when you shut down your PC.

Important updates

Download updates but let me choose whether to install them

- Install updates automatically (recommended)
- Download updates but let me choose whether to install them
- Check for updates but let me choose whether to download and install them

n a metered

Recommended updates

☑ Give me recommended updates the same way I receive important updates

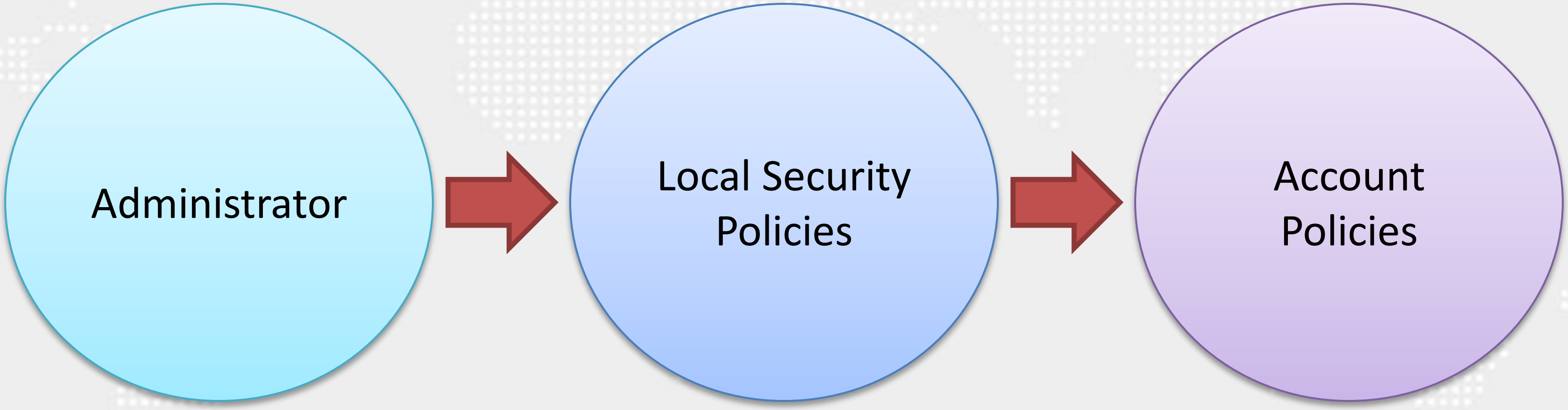
Microsoft Update

□ Give me updates for other Microsoft products when I update Windows

Note: Windows Update might update itself automatically first when checking for other updates. Read our

Security Settings

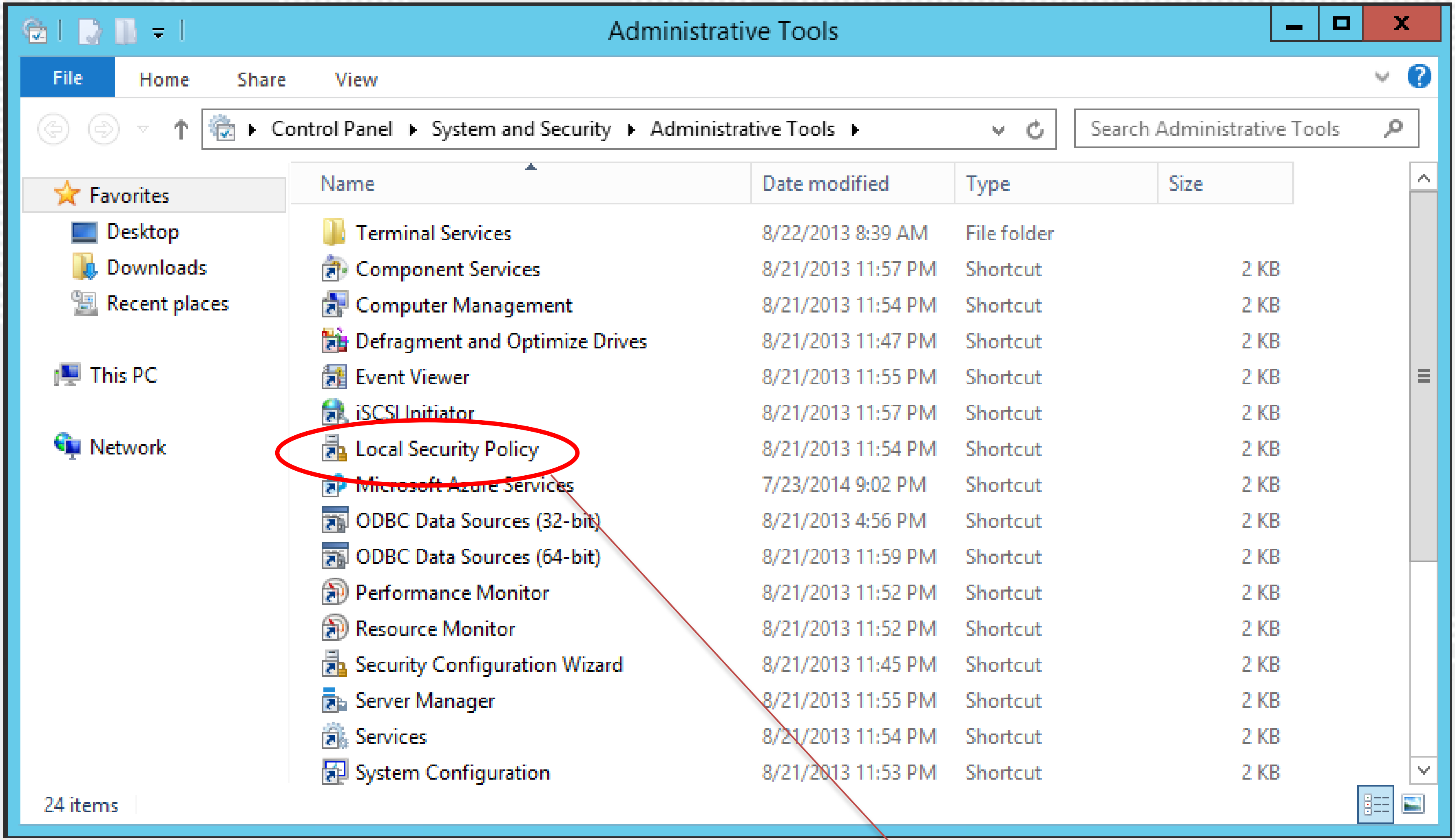
Account Policies



Administrator

Local Security Policies

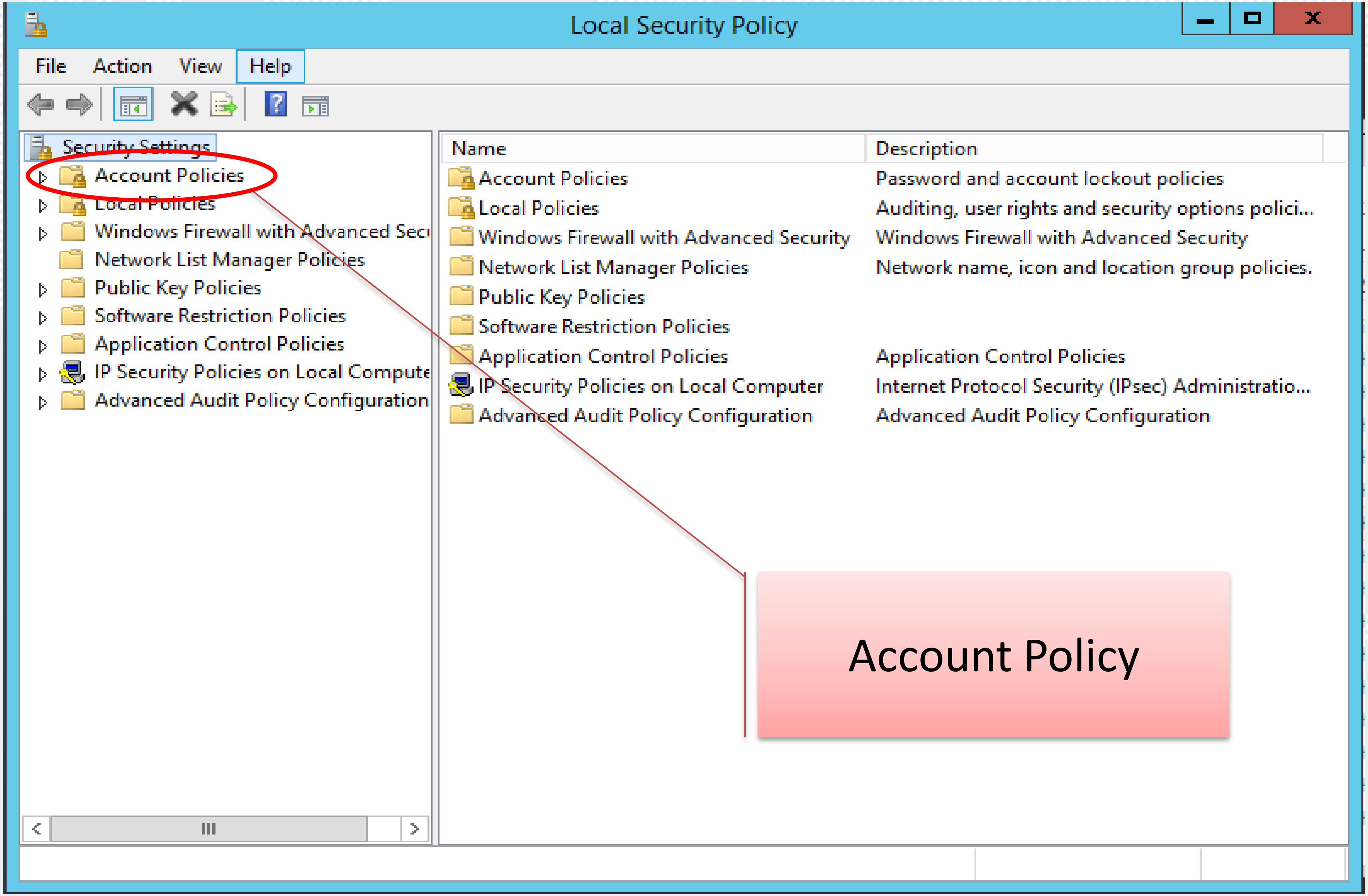
Account Policies



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
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB

24 items

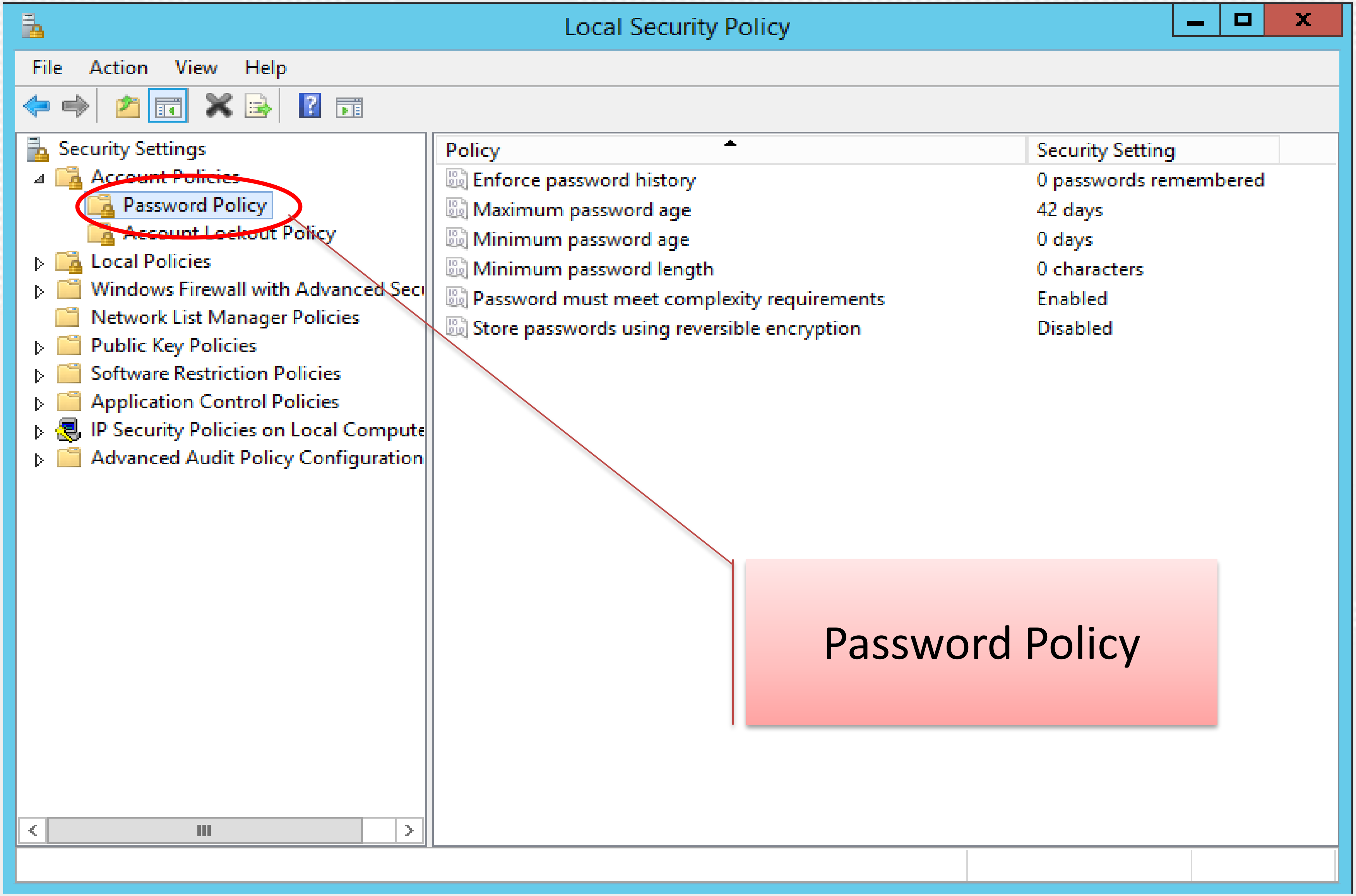
Local Security Policy



Security Settings
- Account Policies
- 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

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



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

Account Policies

Password Policies

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

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

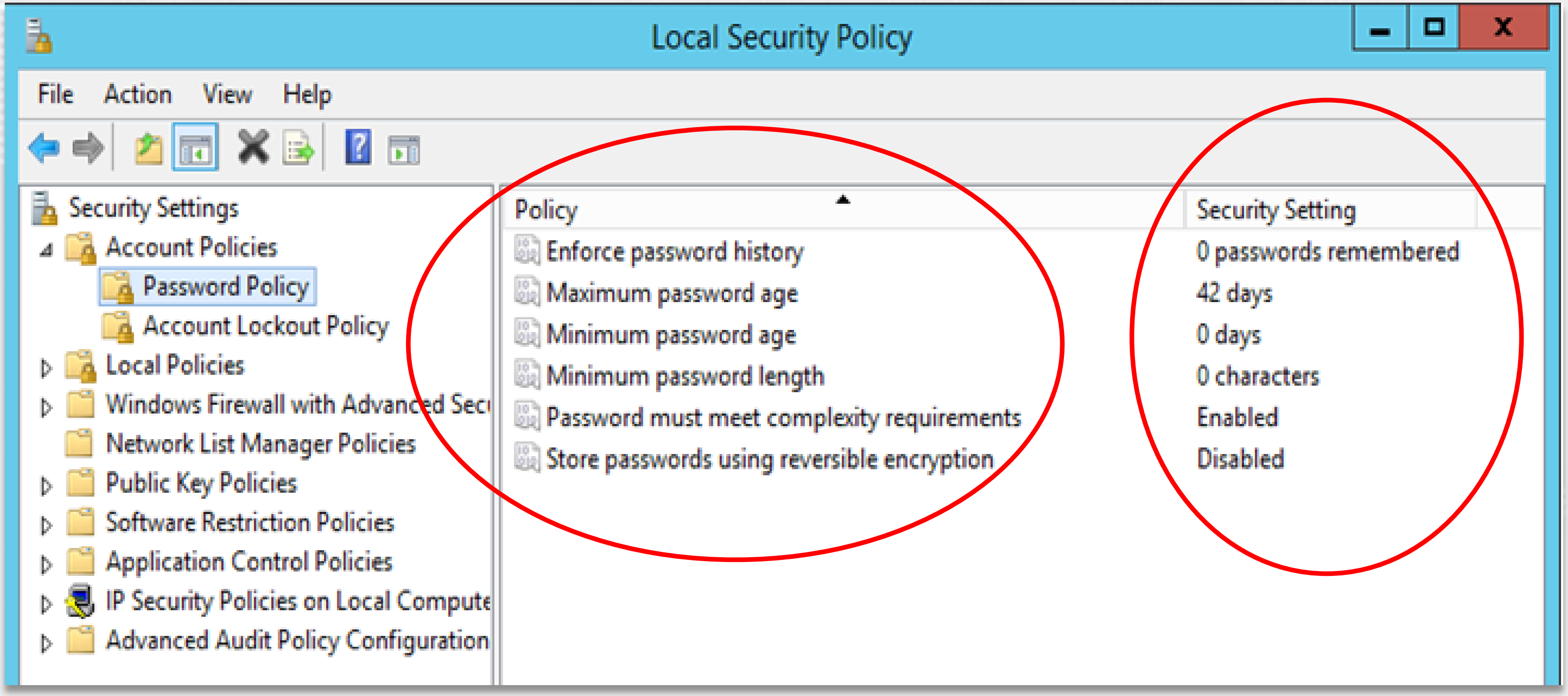
Set 'Password must meet complexity requirements' to 'Enabled‘

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'

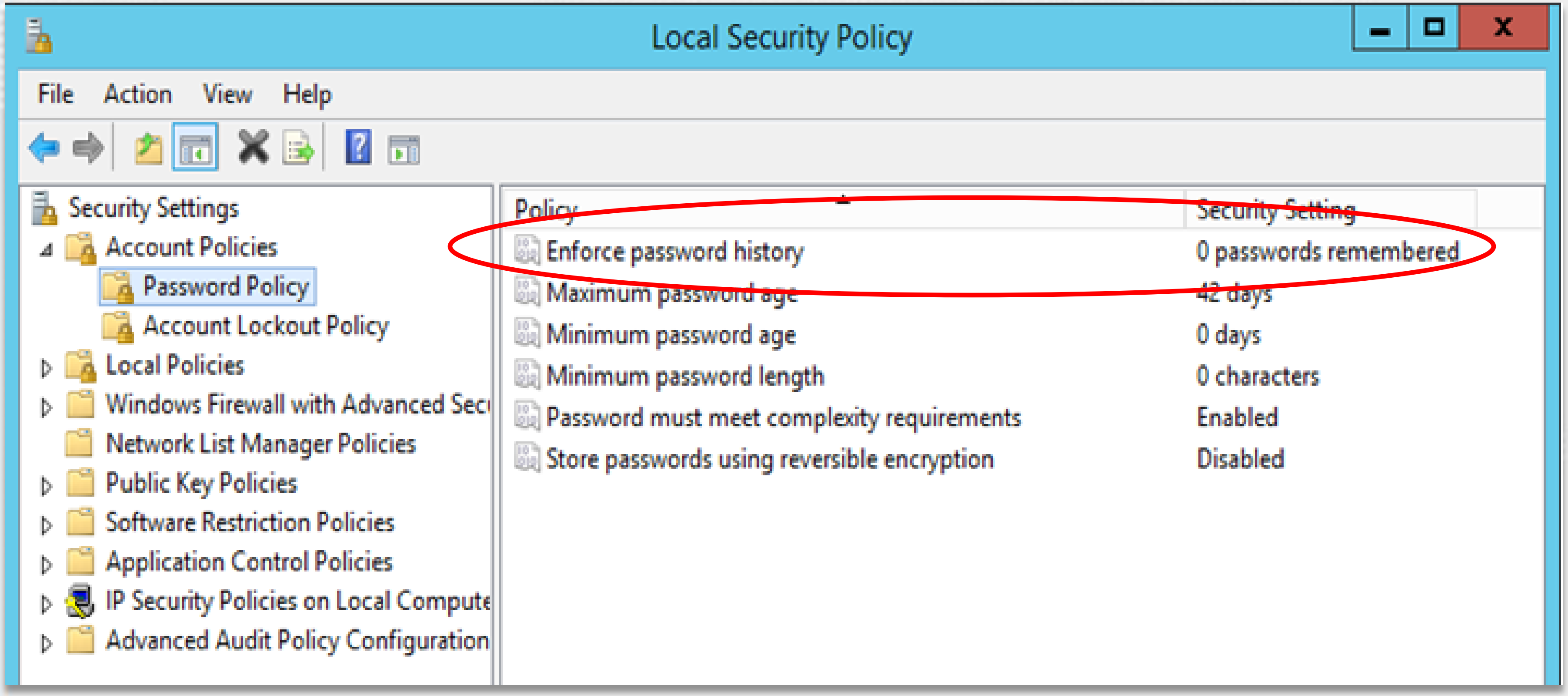
Password Policies


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced 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 Policies

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

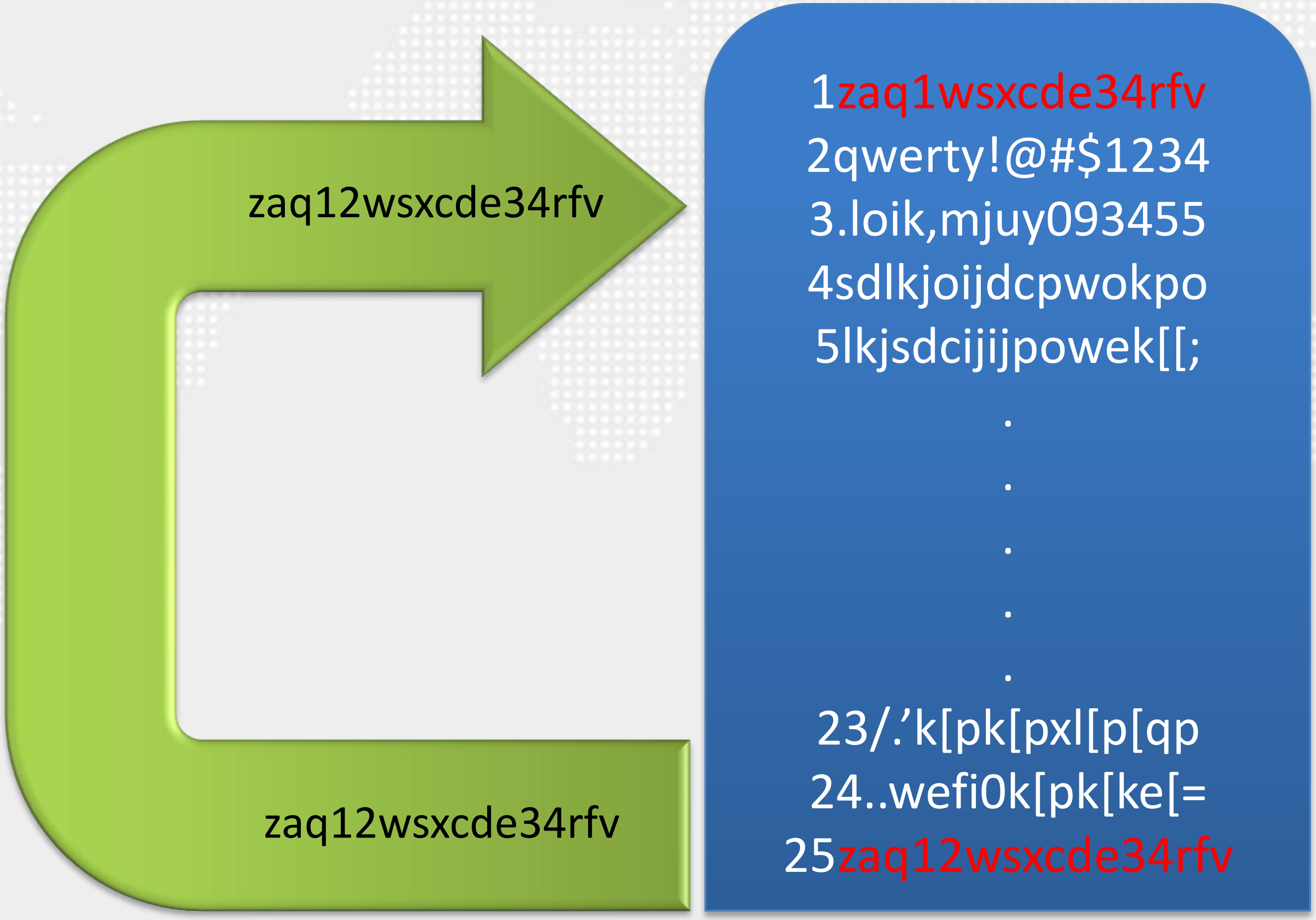


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on 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 Policies

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



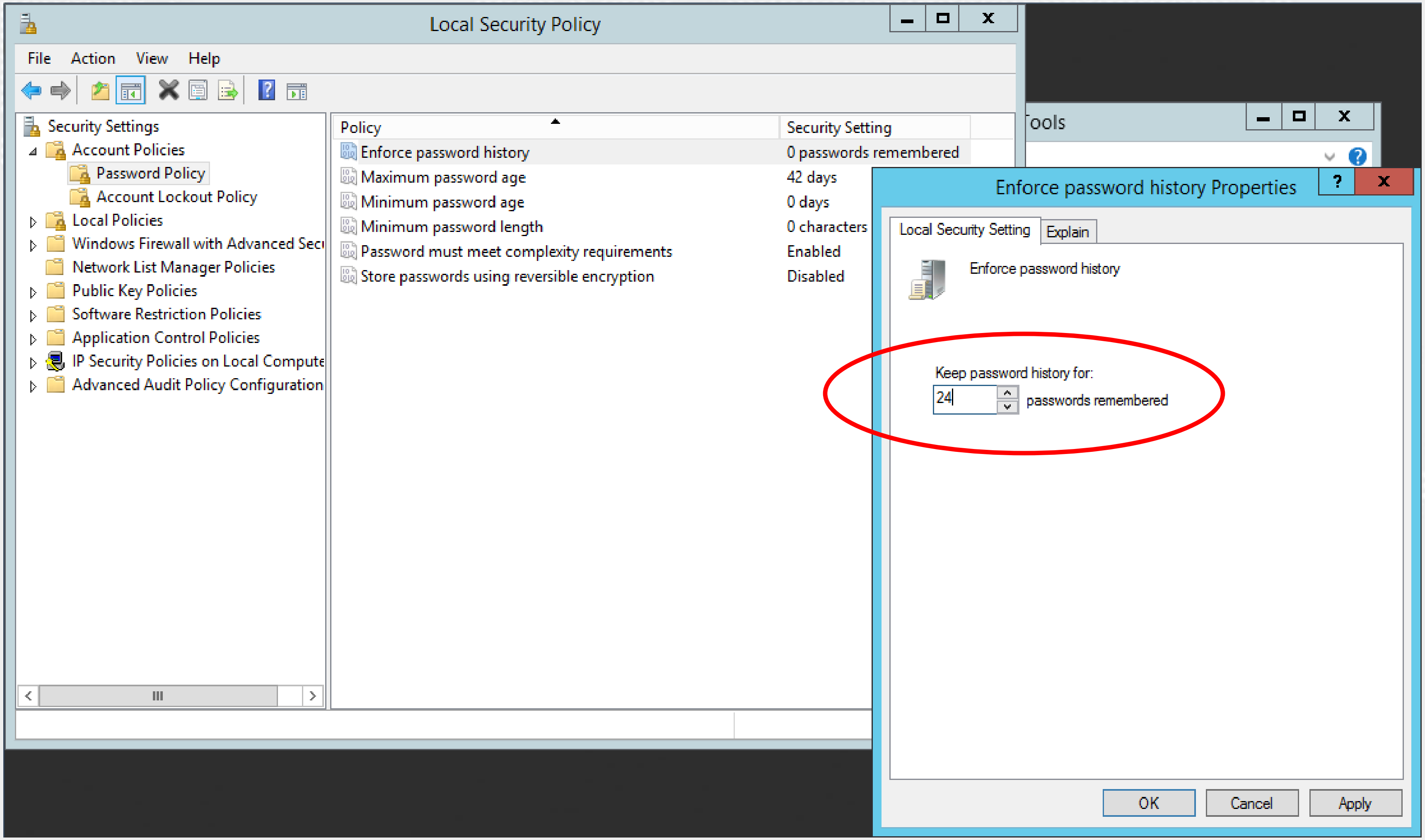
zaq12wsxcde34rfv

zaq12wsxcde34rfv

1zaq1wsxcde34rfv
2qwerty!@#$1234
3.loik,mjuy093455
4sdlkjoijdcpwokpo
5lkjsdcijijpowek[[;
.
.
.
.
.
23/.’k[pk[pxl[p[qp
24..wefi0k[pk[ke[=
25zaq12wsxcde34rfv

Password Policies

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



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
Tools

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

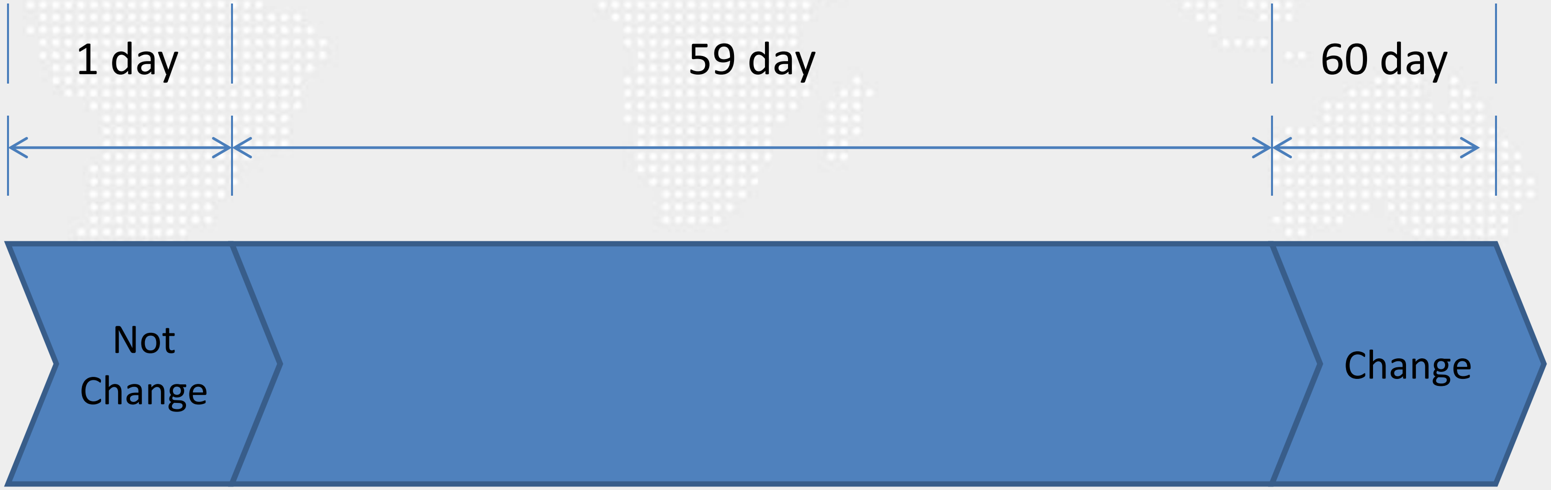
Enforce password history

Keep password history for:
24 passwords remembered

Password Policies

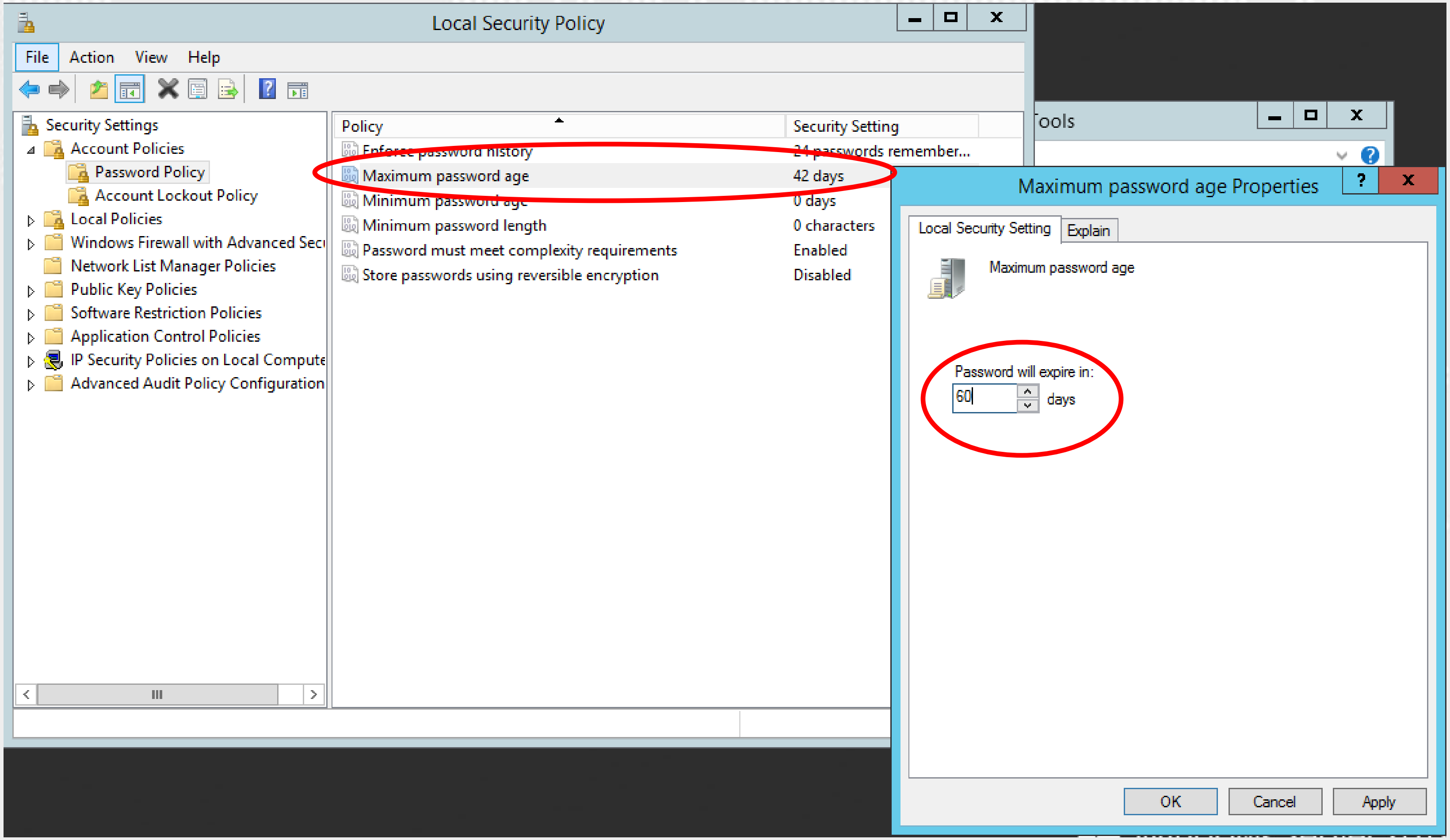
Set 'Minimum password age' to '1 or more day(s)'

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



Password Policies

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



- 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

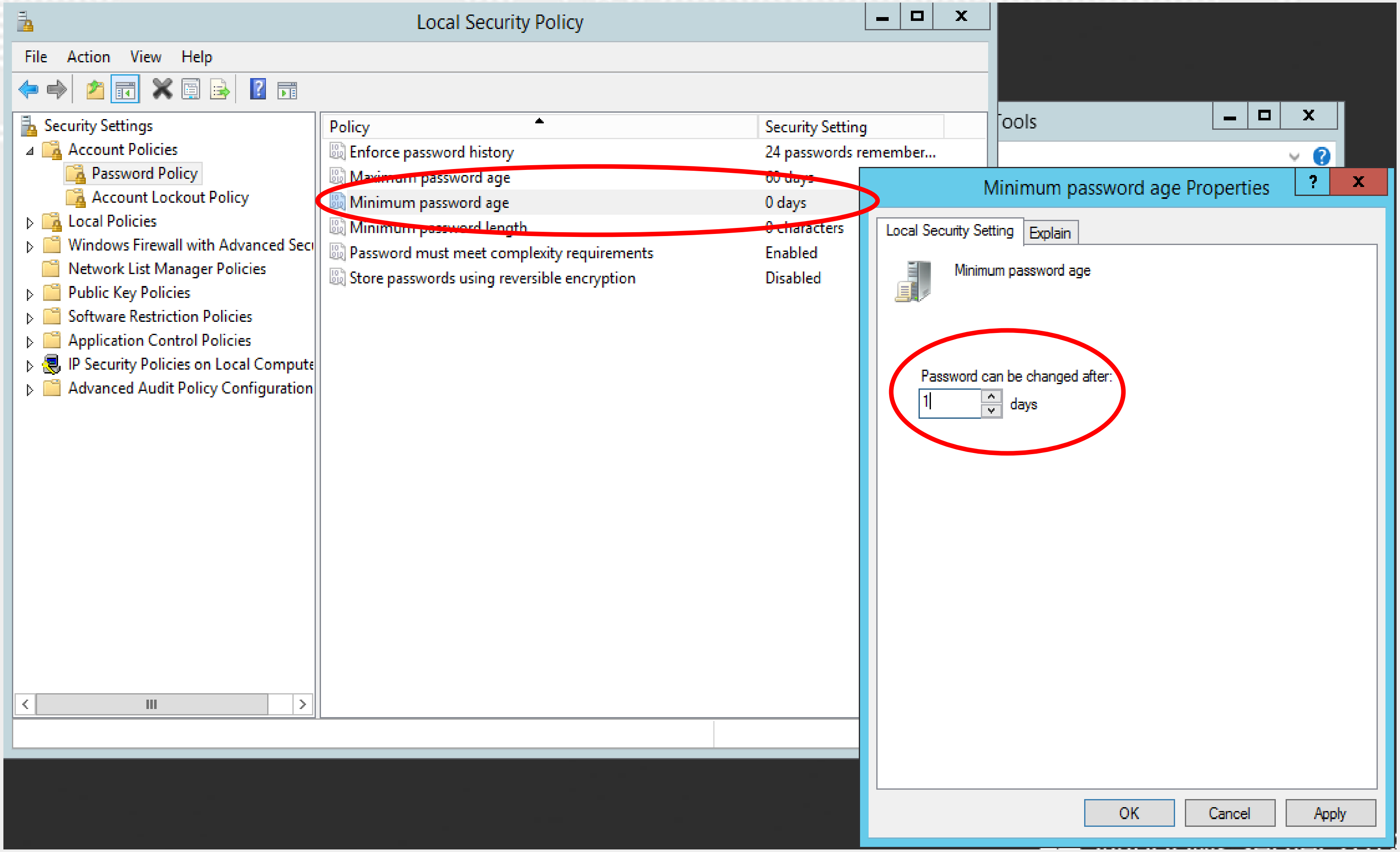
Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Maximum password age

Password will expire in: 60 days

Password Policies

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



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
  - Windows Firewall with Advanced Seci
  - 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	24 passwords remember...
Maximum password age	60 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

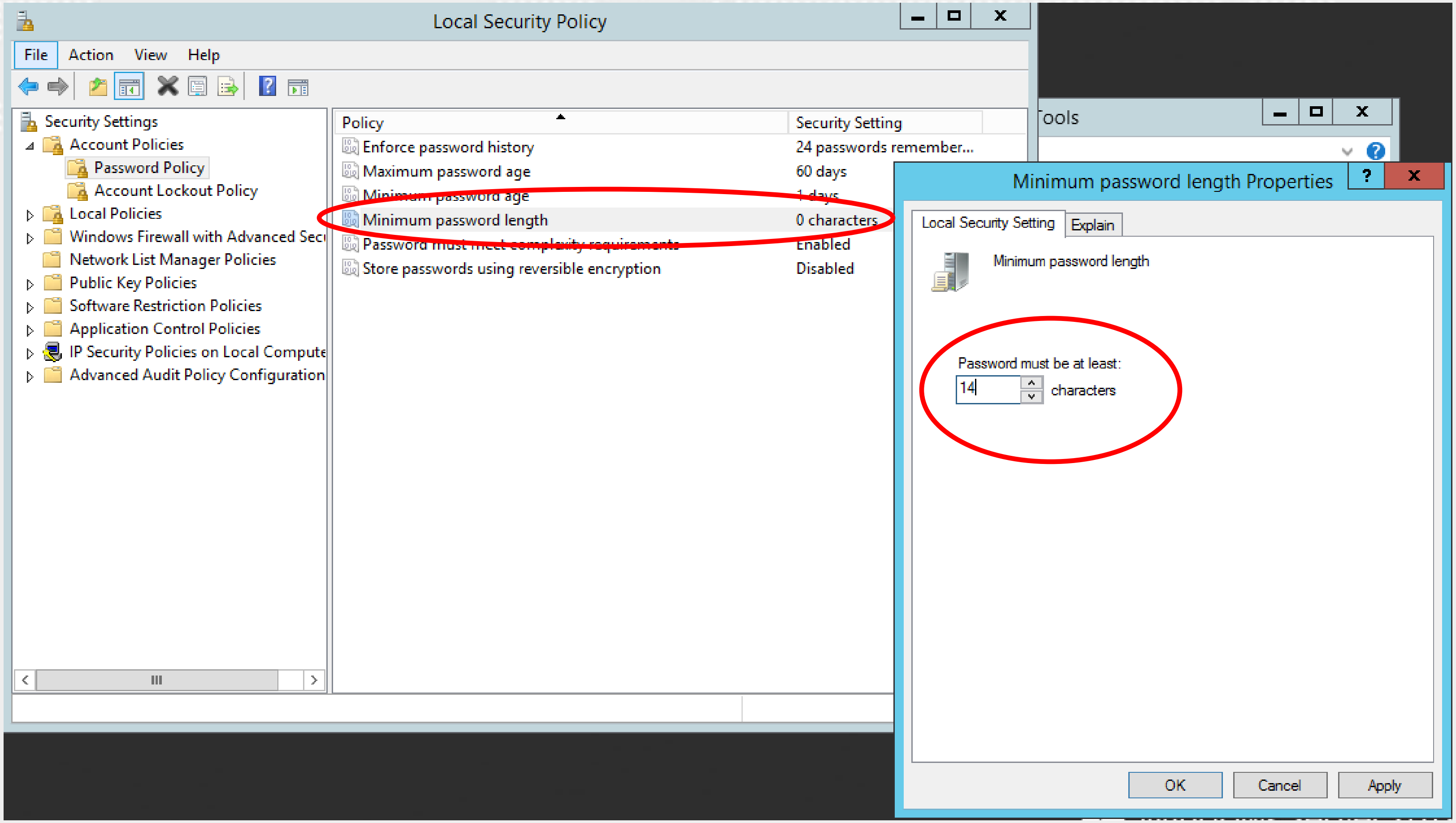
Minimum password age

Password can be changed after:

1 days

Password Policies

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



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
Tools

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

Minimum password length Properties

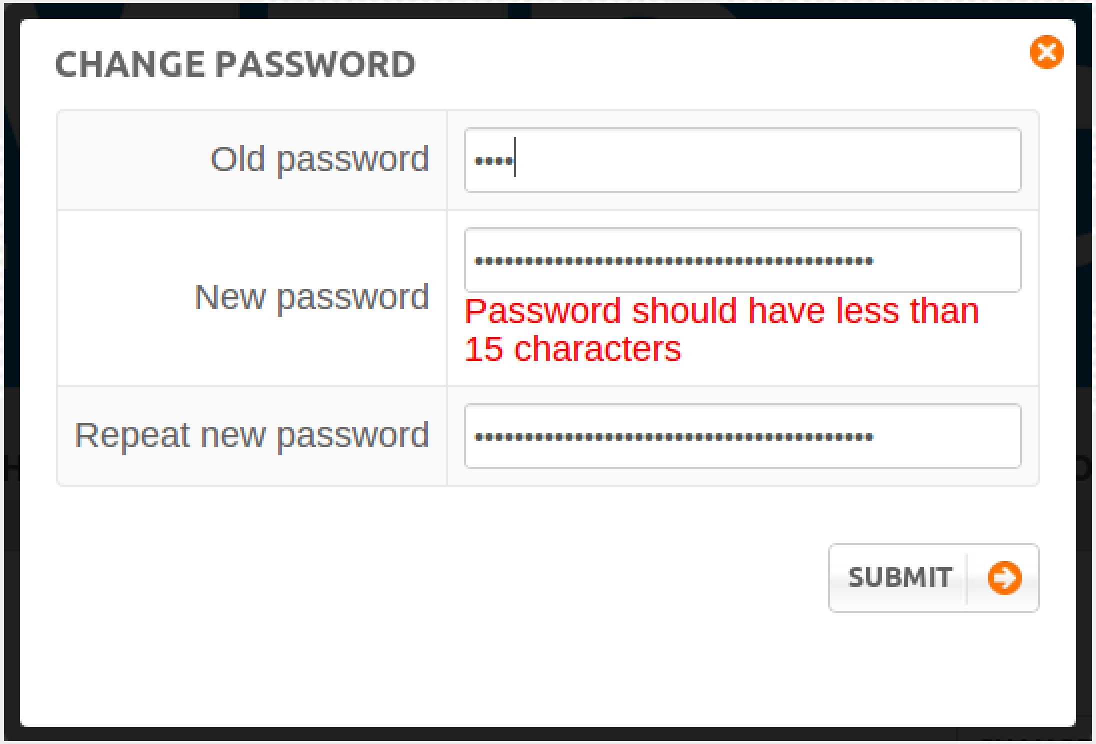
Local Security Setting
Explain

Minimum password length

Password must be at least:
14 characters

Password Policies

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



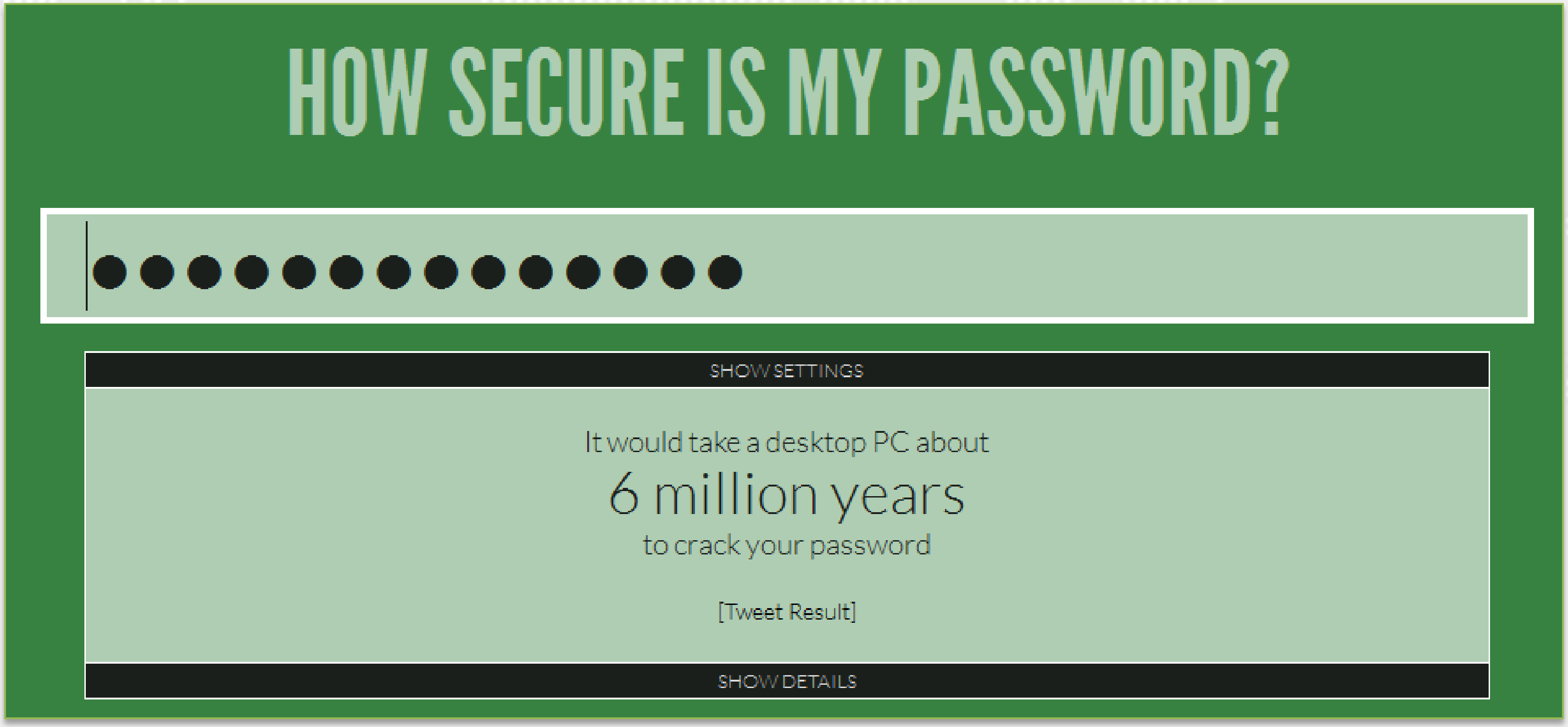
CHANGE PASSWORD

Old password	••••
New password	•• Password should have less than 15 characters
Repeat new password	••

Password Policies

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

https://howsecureismypassword.net/



HOW SECURE IS MY PASSWORD?

●●●●●●●●●●●●●●

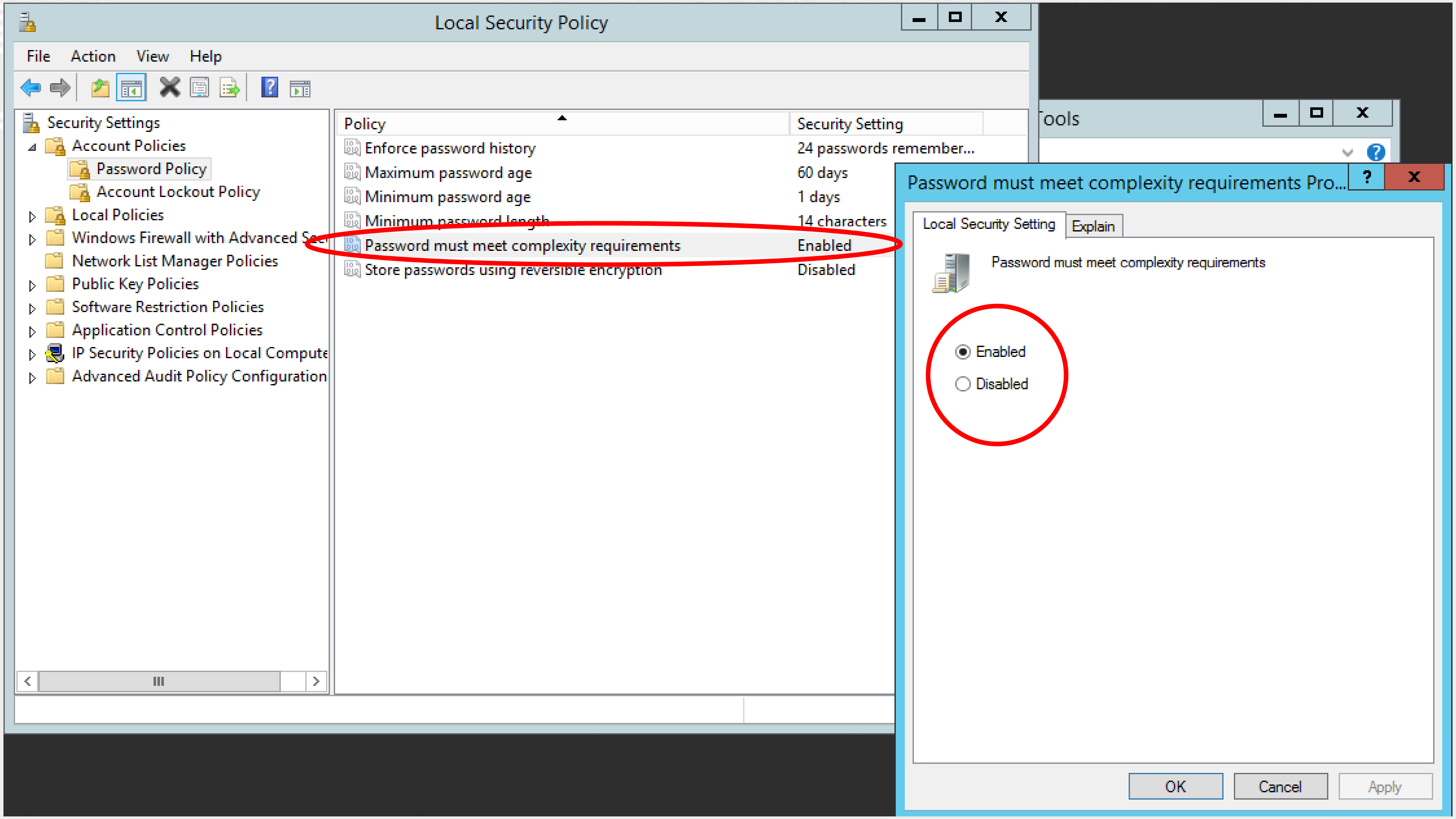
It would take a desktop PC about

6 million years

to crack your password

Password Policies

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



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Se...
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Tools
Password must meet complexity requirements Pro...
Local Security Setting
Explain
OK
Cancel
Apply

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Password must meet complexity requirements

● Enabled

○ Disabled

Password Policies

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

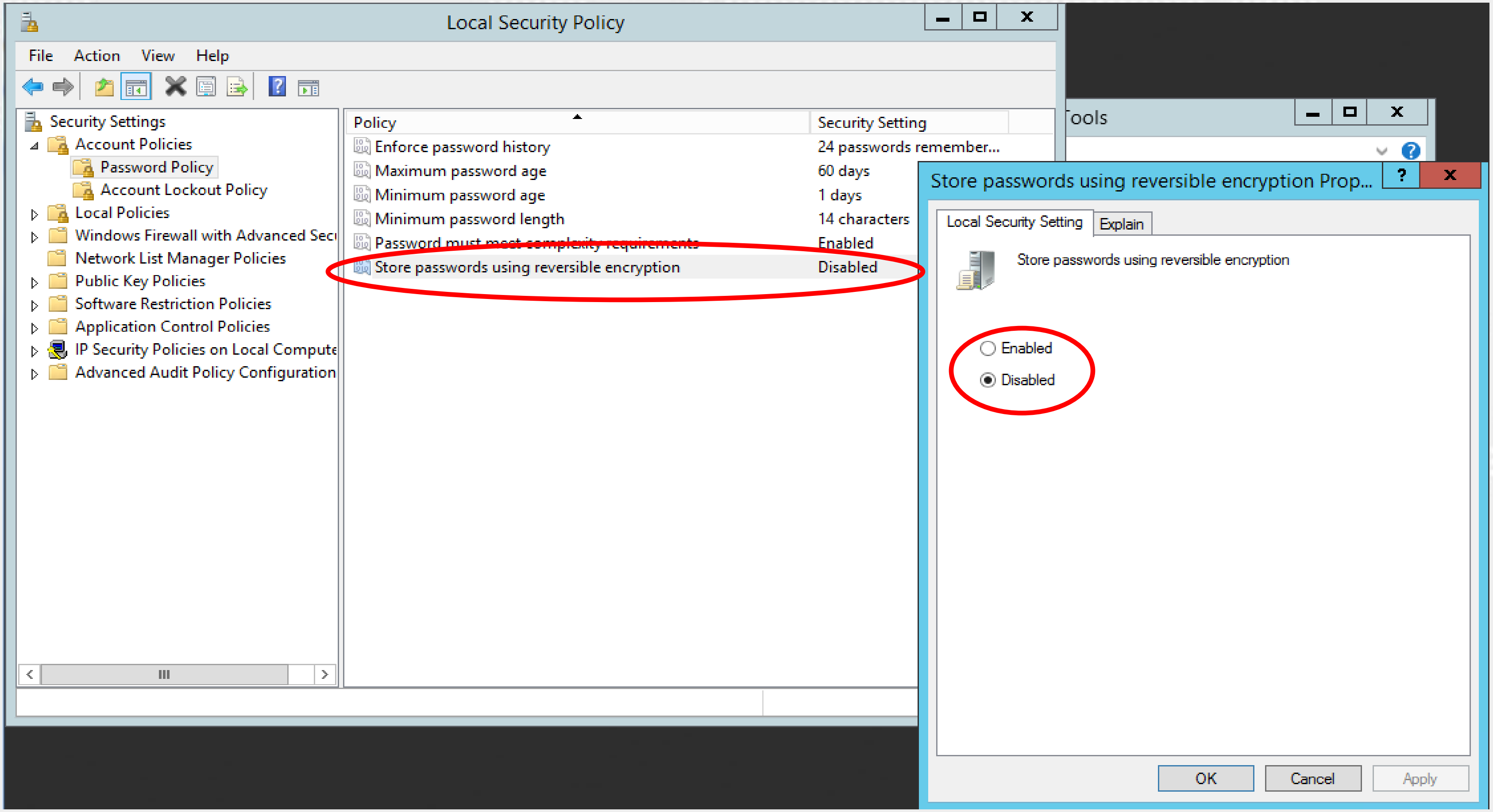
English uppercase characters (A through Z)
English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)

‘kov[I,soj;p’ko4k8iy{

งานอบรมหน่วยงานภาครัฐ

Password Policies

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



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
Tools
Store passwords using reversible encryption Prop...
Local Security Setting
Explain
OK
Cancel
Apply

Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Store passwords using reversible encryption

○ Enabled

● Disabled

Password Policies

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

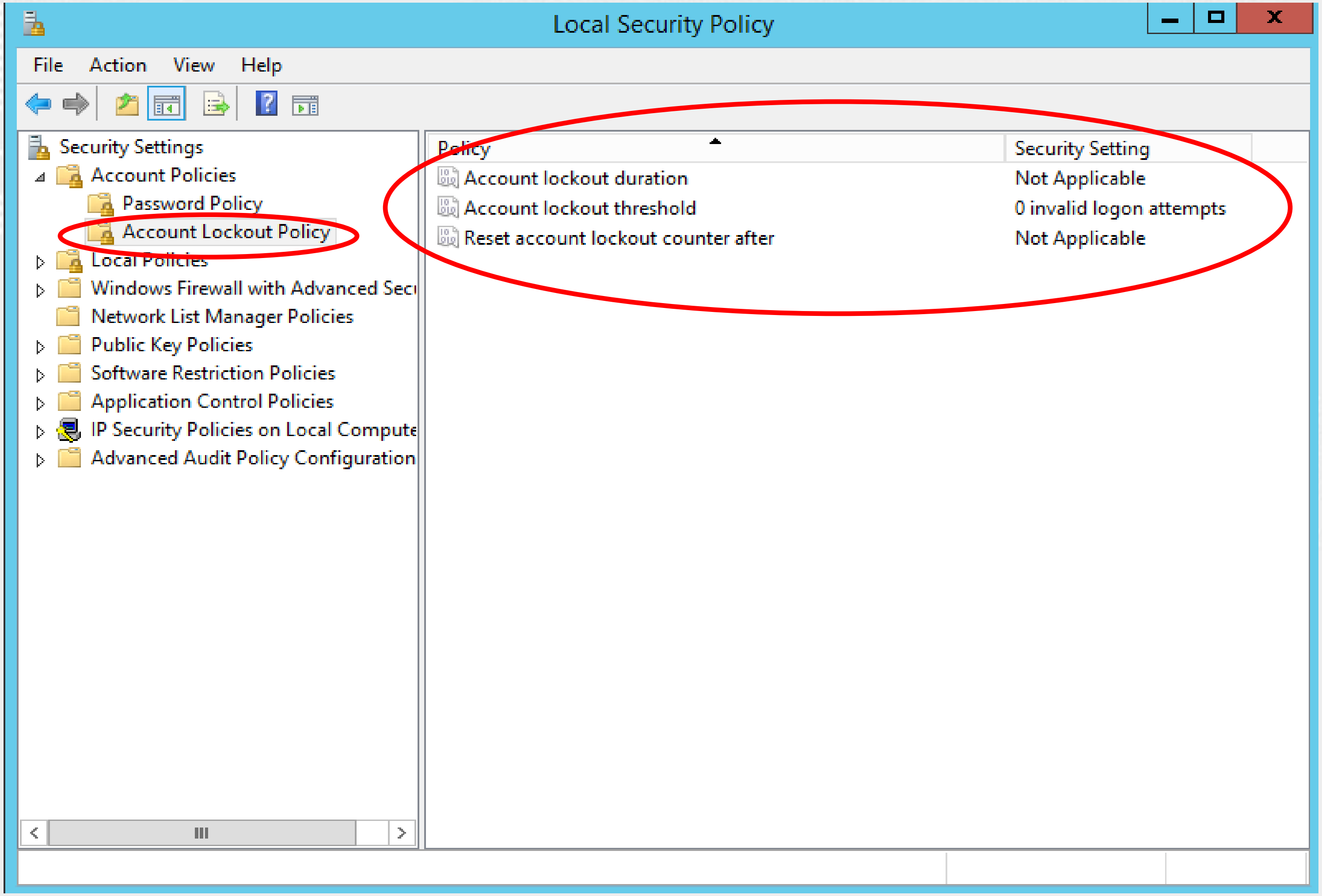
Account Lockout Policy

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

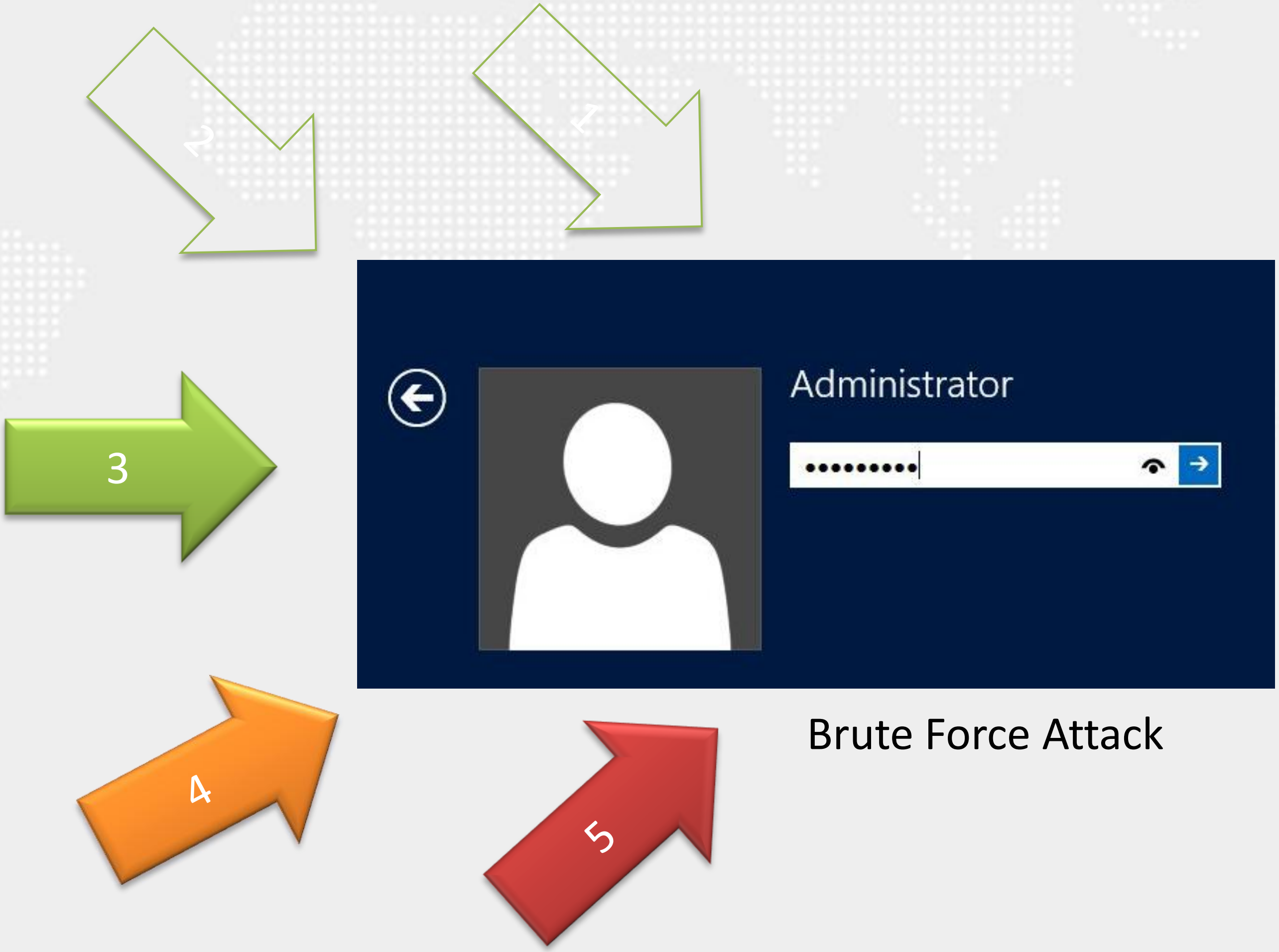


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on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

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

Account Lockout Policy

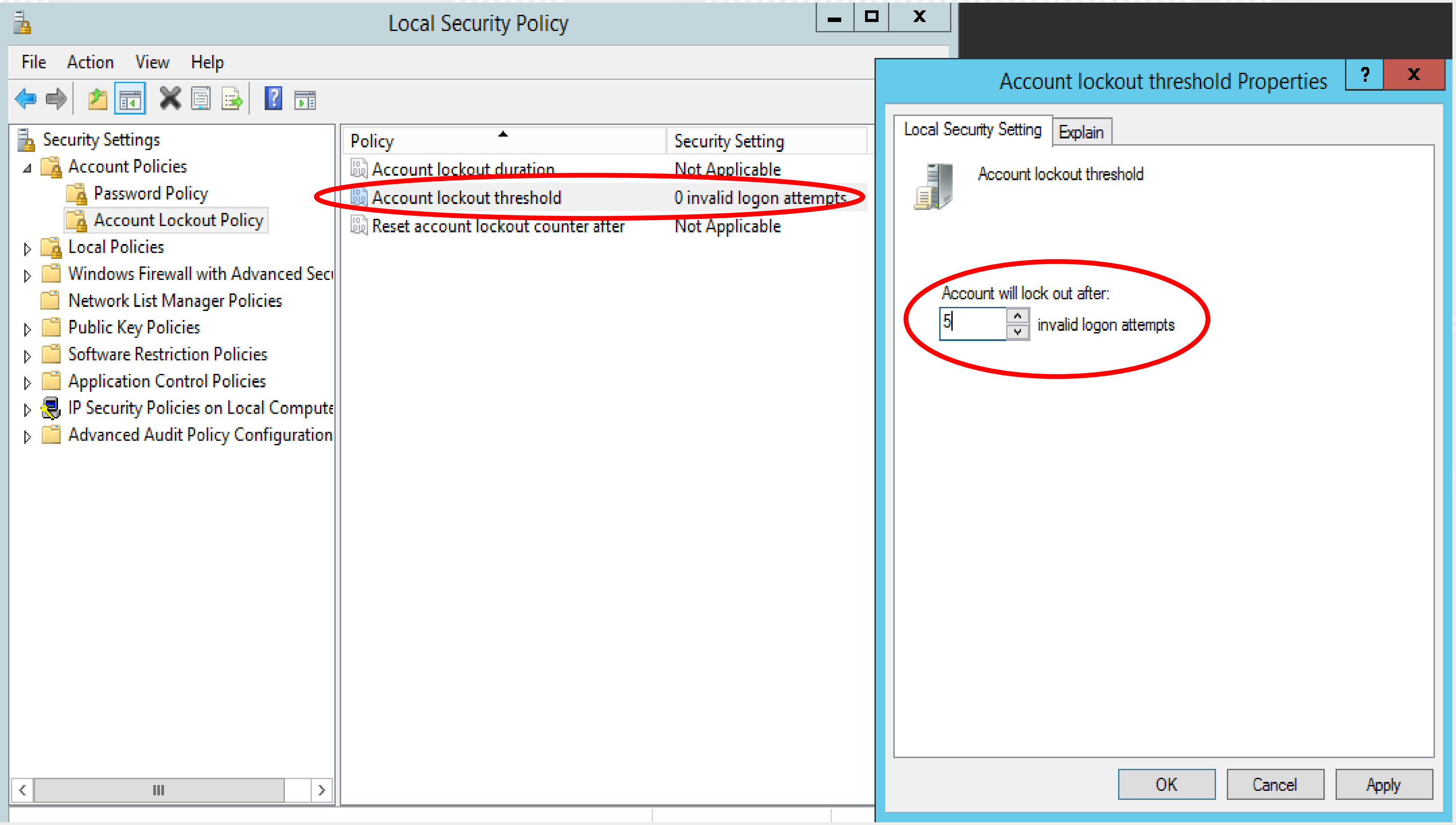
Set 'Account lockout threshold' to '5 invalid logon attempt(s)'



Brute Force Attack

Account Lockout Policy

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



- 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
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

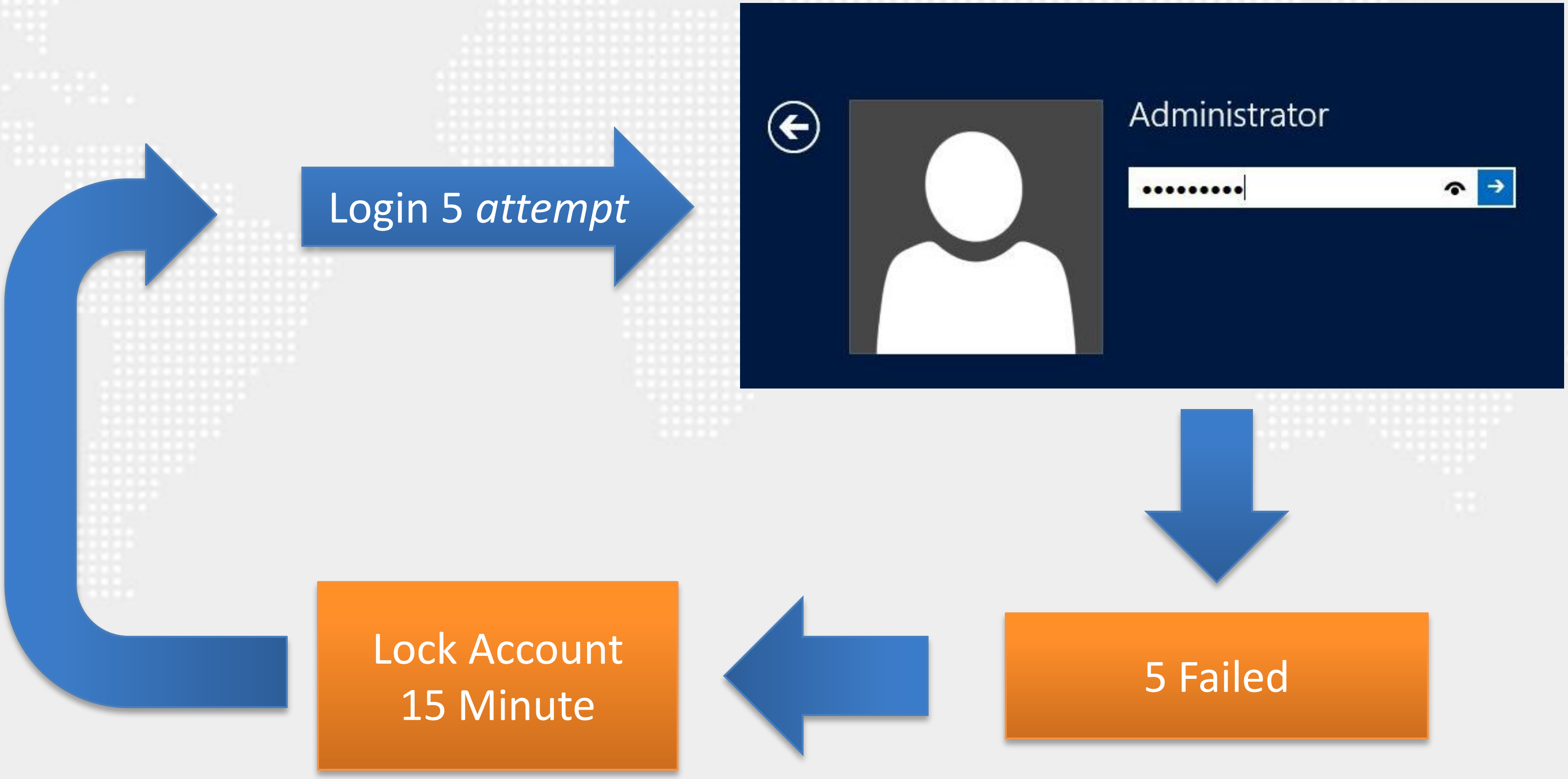
Account lockout threshold

Account will lock out after:

5 invalid logon attempts

Account Lockout Policy

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

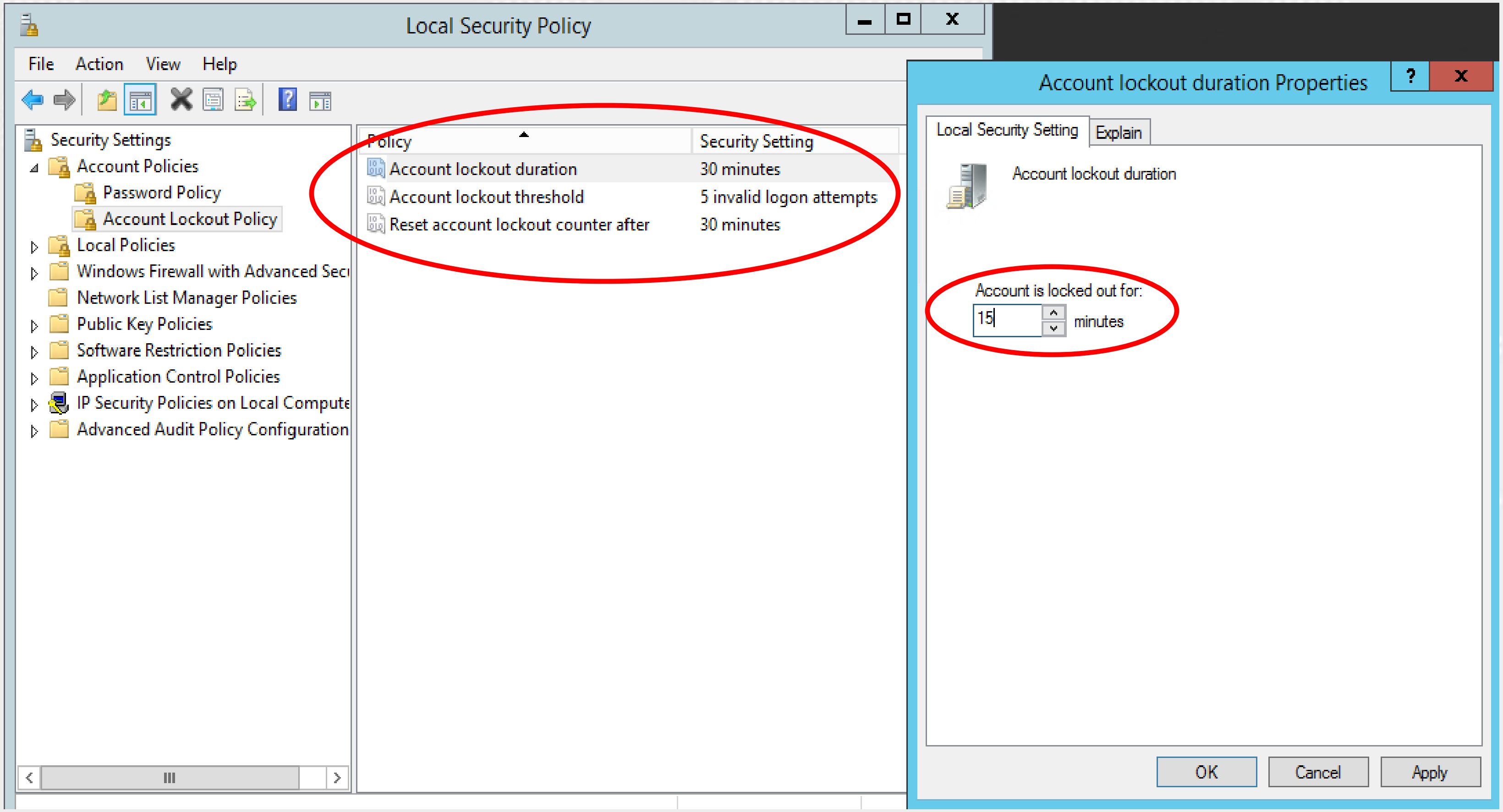


** ‘0’ Administrator unlock manually*

http://www.cisecurity.org/

Account Lockout Policy

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



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
Account lockout duration Properties
Local Security Setting
Explain
OK
Cancel
Apply

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Account lockout duration

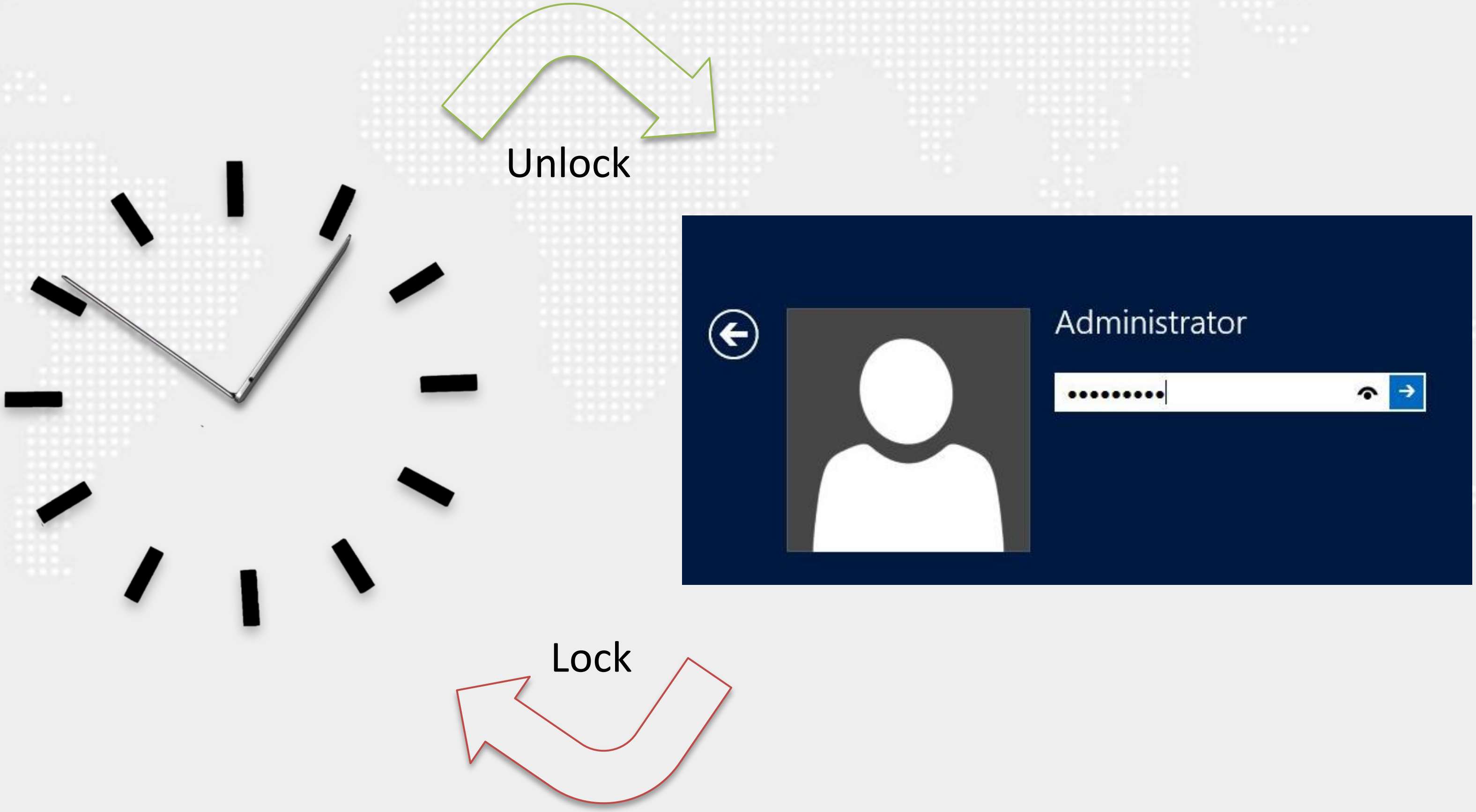
Account is locked out for:

15 minutes

** '0' Administrator unlock manually*

Account Lockout Policy

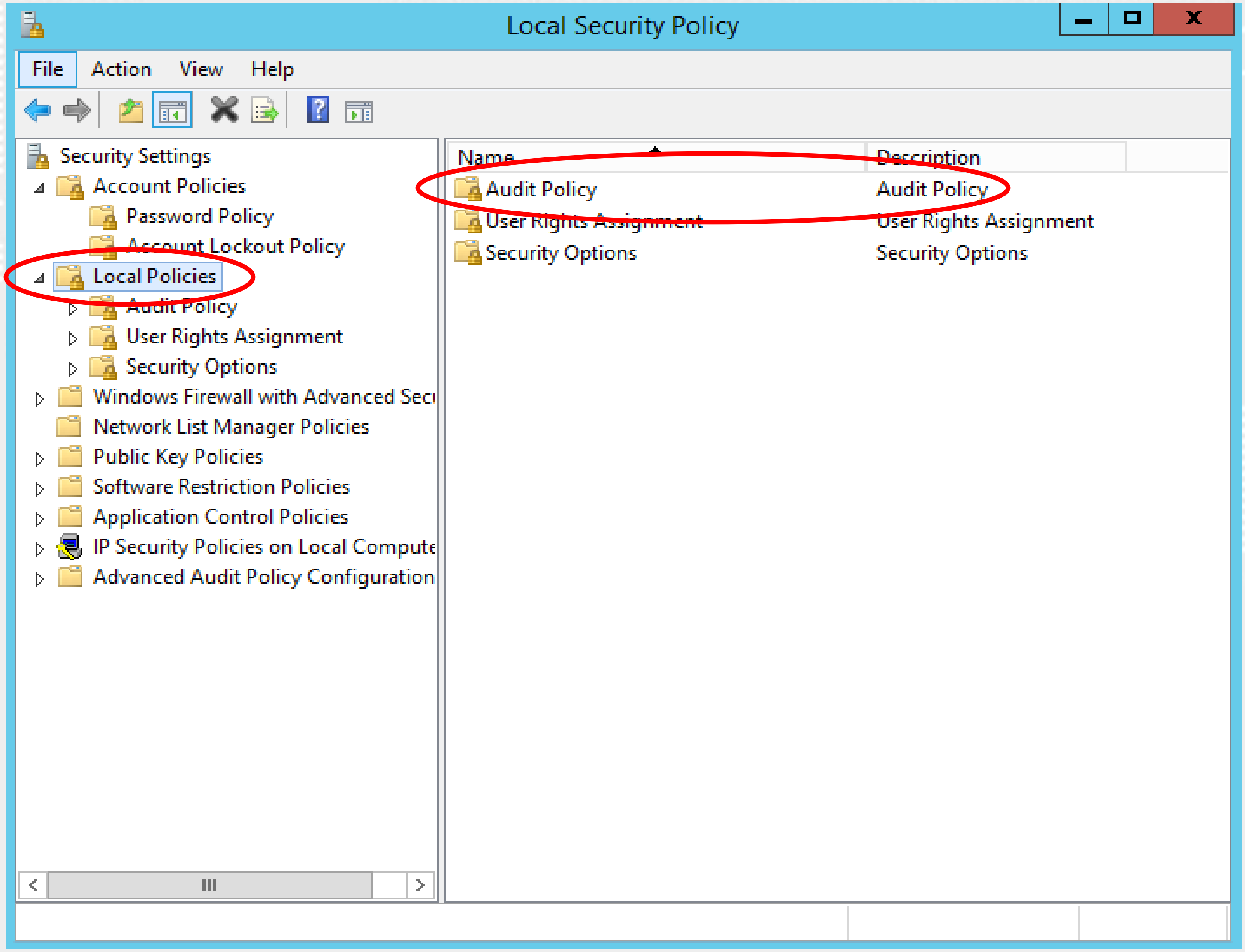
Set 'Reset account lockout counter after' to '15 minute(s)'



Unlock

Lock

Advanced Audit Policy Configuration


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

Name	Description
Audit Policy	Audit Policy
User Rights Assignment	User Rights Assignment
Security Options	Security Options

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'

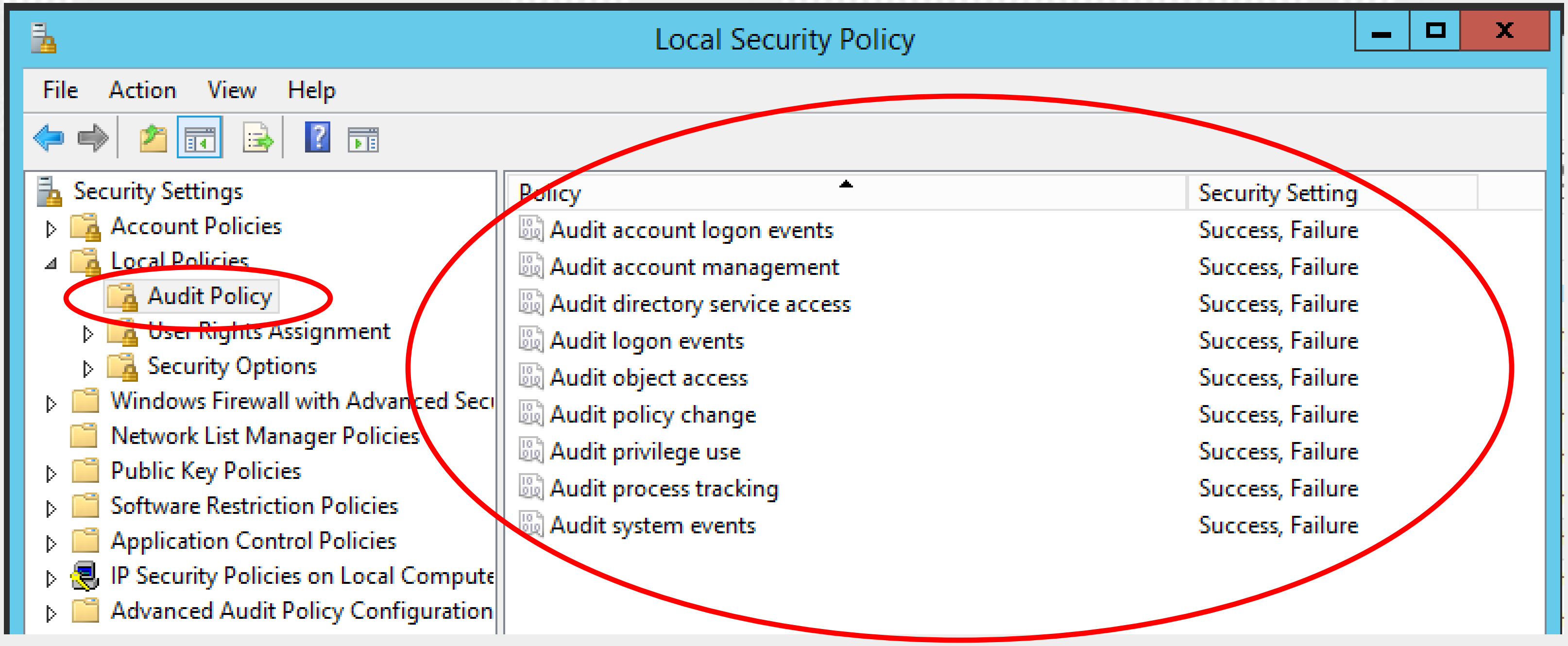
Set 'Audit Policy: System: Security State Change' to 'Success and Failure'

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

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

Advanced Audit Policy Configuration

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

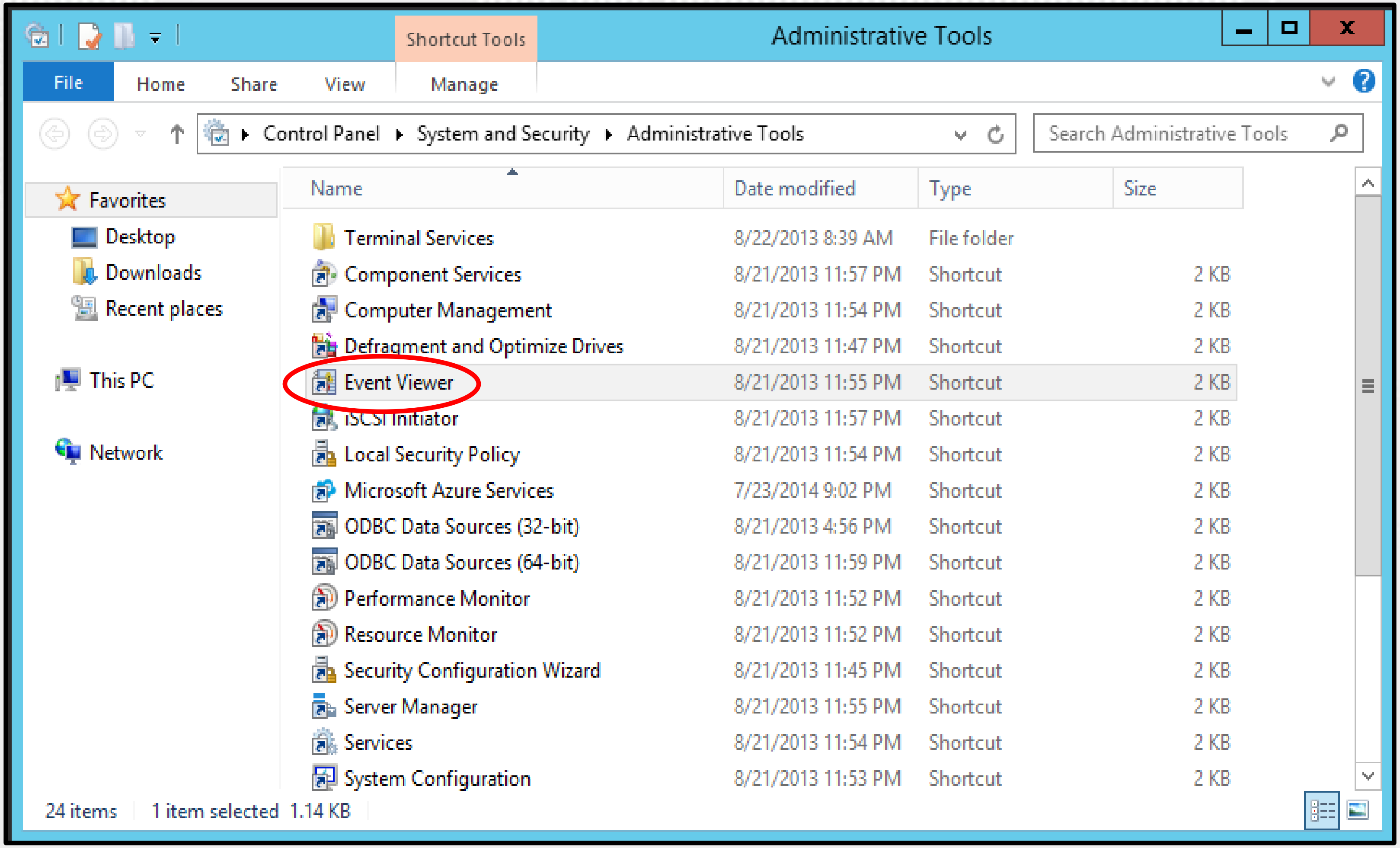


- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP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

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Event Log (Event Viewer)

Control Panel\System and Security\Administrative Tools

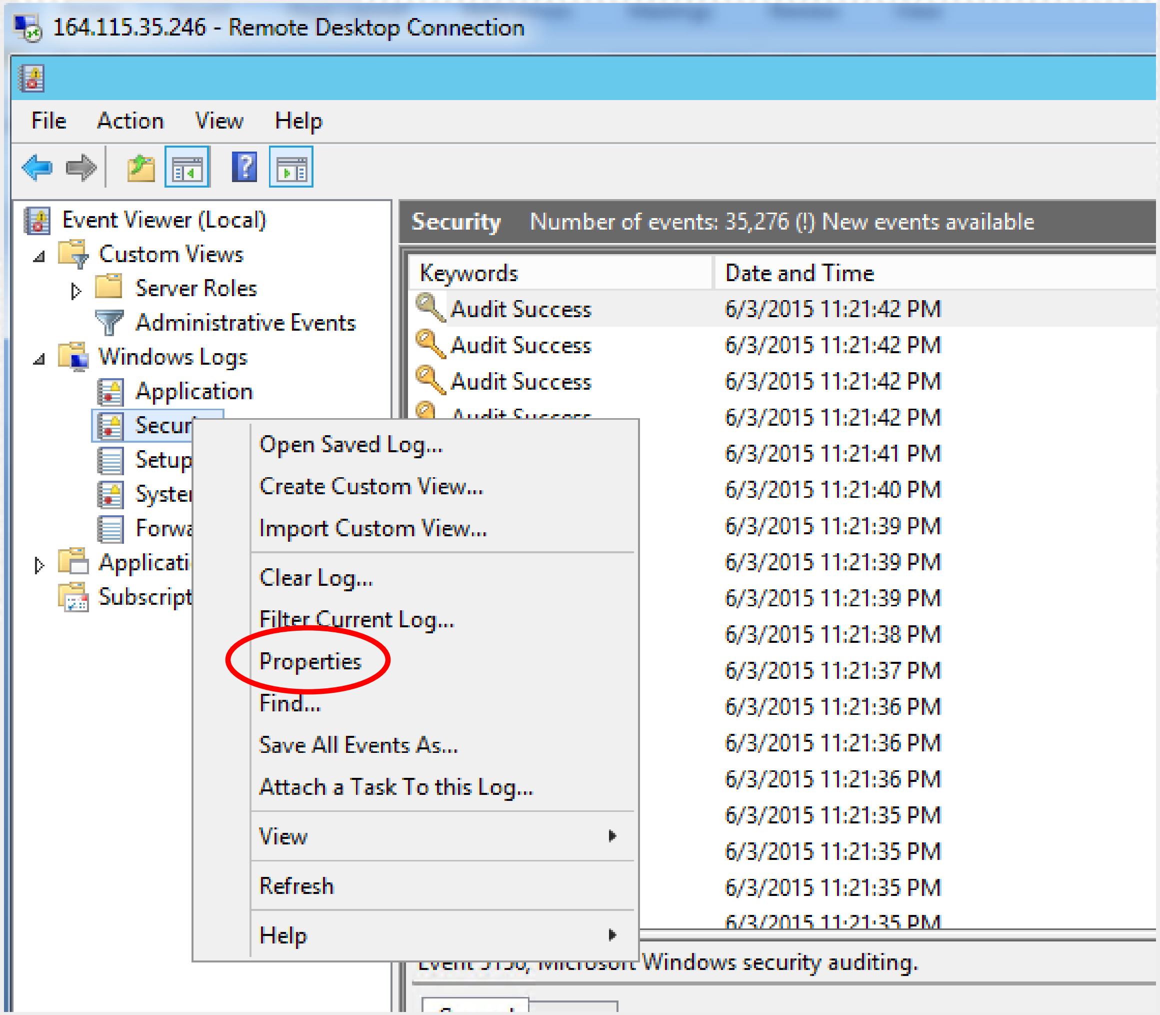


Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
iSCSI Initiator	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
Services	8/21/2013 11:54 PM	Shortcut	2 KB
System Configuration	8/21/2013 11:53 PM	Shortcut	2 KB

24 items   1 item selected 1.14 KB

Event Log (Event Viewer)

Set Maximum Log Size (KB)



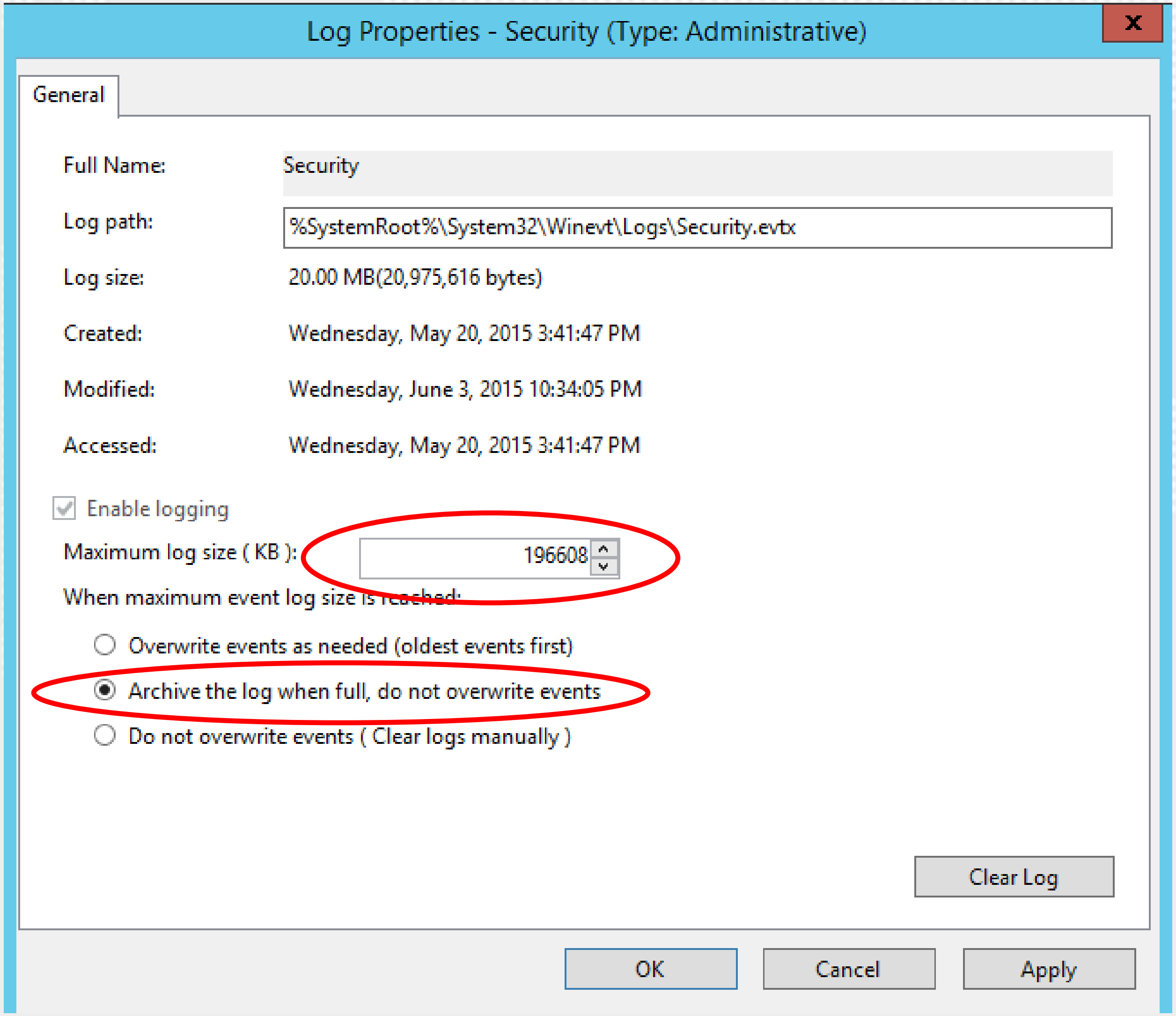
Security Number of events: 35,276 (!) New events available

Keywords	Date and Time
Audit Success	6/3/2015 11:21:42 PM
Audit Success	6/3/2015 11:21:42 PM
Audit Success	6/3/2015 11:21:42 PM
Audit Success	6/3/2015 11:21:42 PM
	6/3/2015 11:21:41 PM
	6/3/2015 11:21:40 PM
	6/3/2015 11:21:39 PM
	6/3/2015 11:21:39 PM
	6/3/2015 11:21:39 PM
	6/3/2015 11:21:38 PM
	6/3/2015 11:21:37 PM
	6/3/2015 11:21:36 PM
	6/3/2015 11:21:36 PM
	6/3/2015 11:21:36 PM
	6/3/2015 11:21:35 PM
	6/3/2015 11:21:35 PM
	6/3/2015 11:21:35 PM
	6/3/2015 11:21:35 PM

Event 5156, Microsoft Windows security auditing.

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:

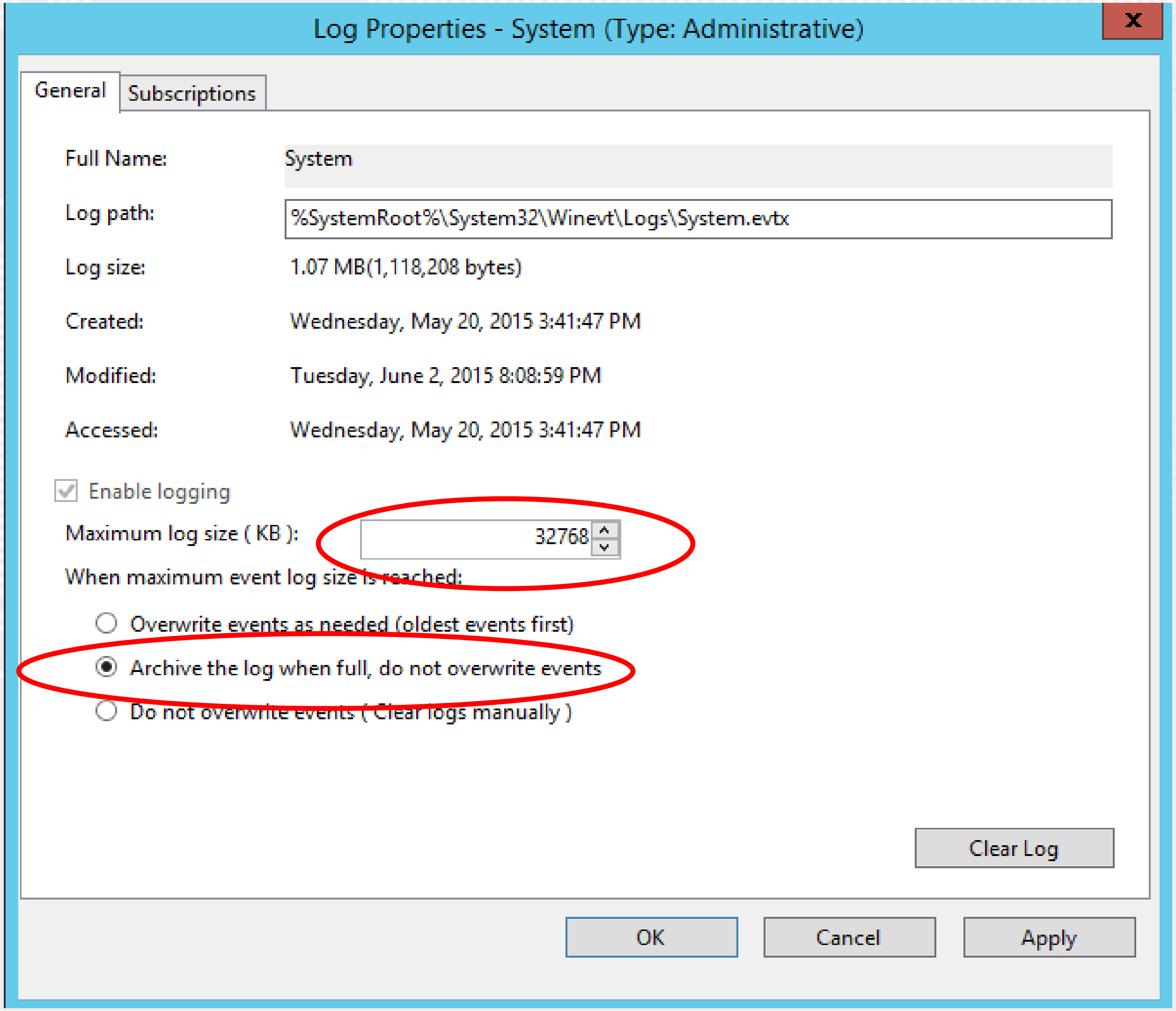
○ Overwrite events as needed (oldest events first)

● Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

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:

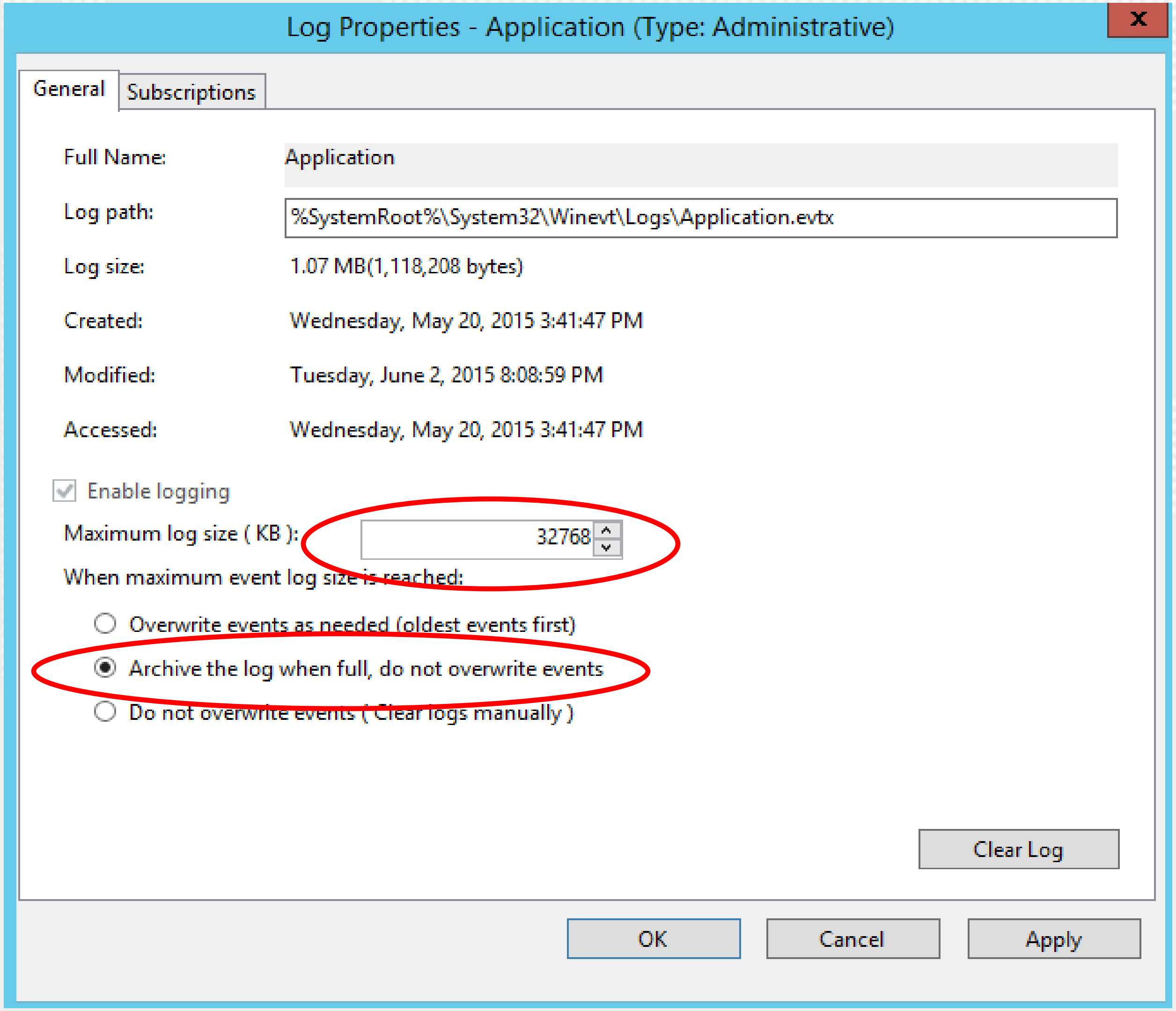
○ Overwrite events as needed (oldest events first)

● Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

Event Log (Event Viewer)

Set 'Application: Maximum Log Size (KB)' to 'Enabled:**_32768_** or greater' (Scored)



Log Properties - Application (Type: Administrative)

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)

Event Log (Event Viewer)

Summery

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

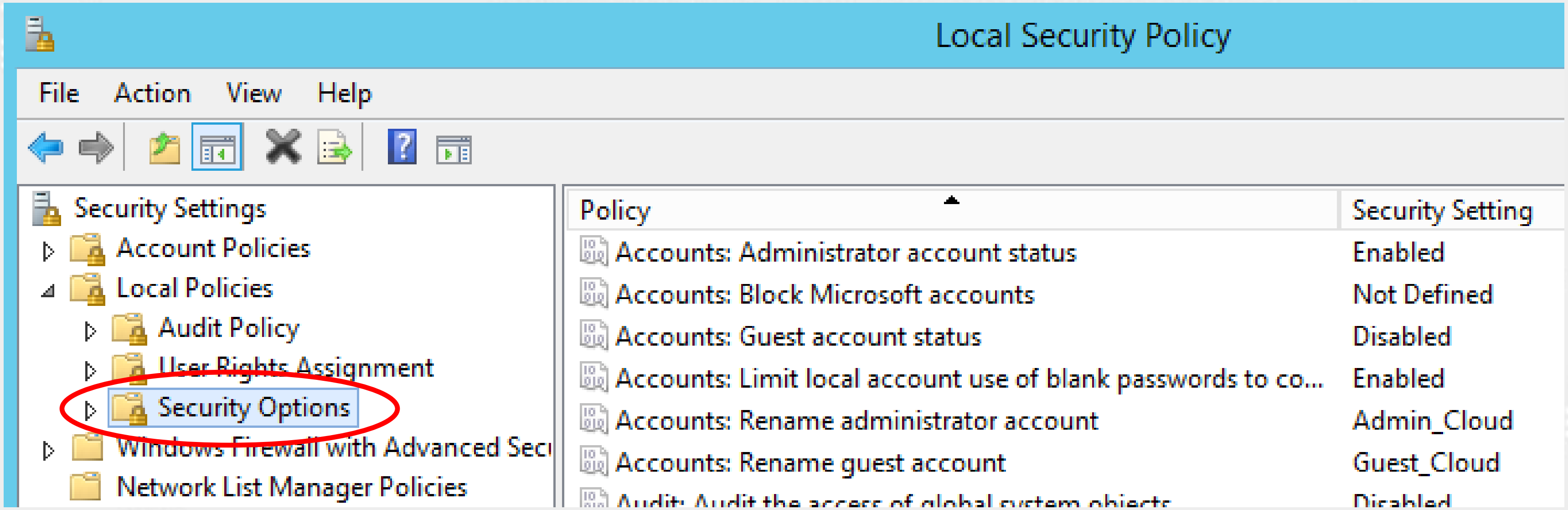
Minimum log file size 1 MB

Maximum log file size 2 TB (2147483647 KB)

MS Windows Server 2012

Security Options

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



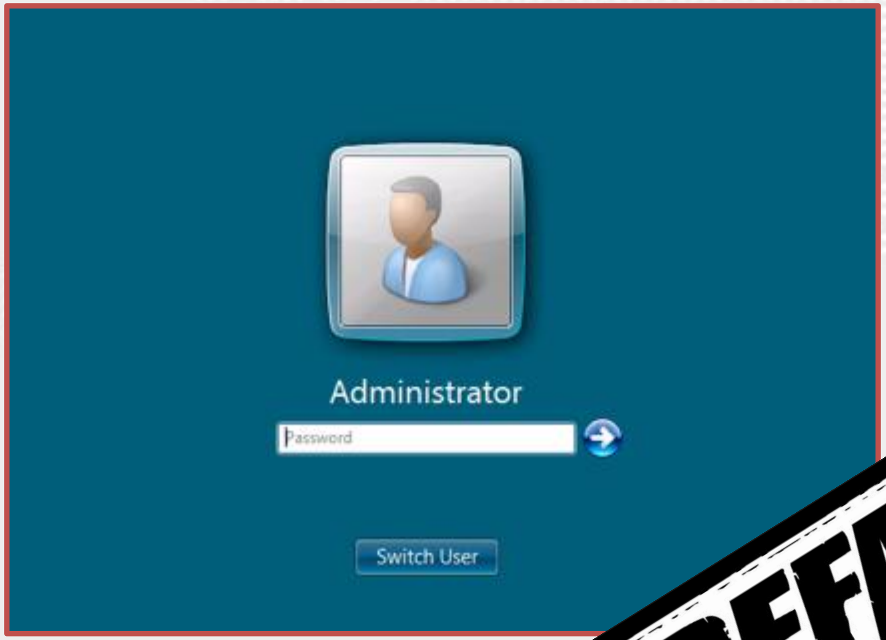
- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies

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

MS Windows Server 2012

Security Options

Configure 'Accounts: Rename administrator account'



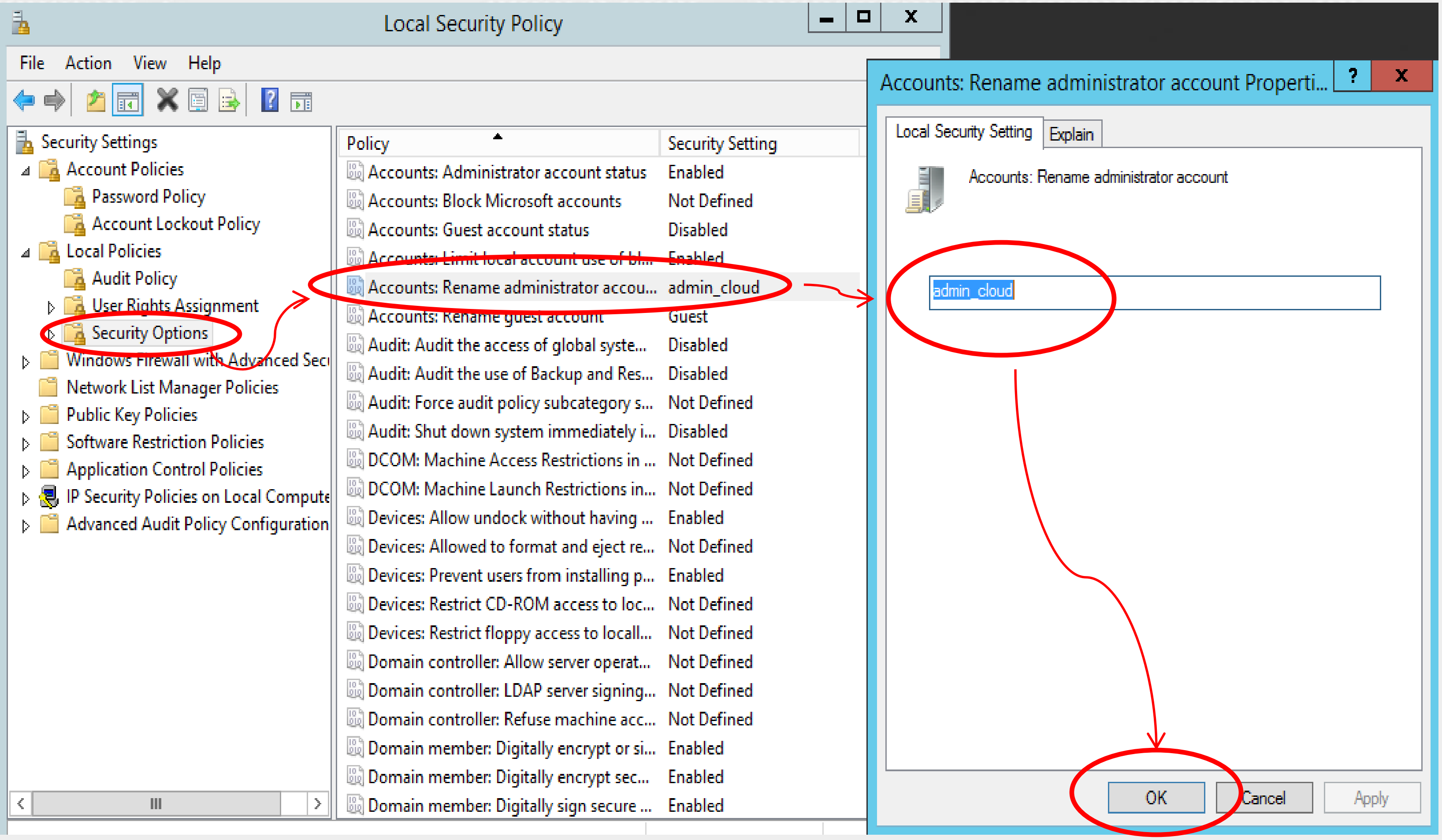
Administrator

DEFAULT

MS Windows Server 2012

Security Options

Configure 'Accounts: Rename administrator account'



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

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of bl...	Enabled
Accounts: Rename administrator accou...	admin_cloud
Accounts: Rename guest account	Guest
Audit: Audit the access of global syste...	Disabled
Audit: Audit the use of Backup and Res...	Disabled
Audit: Force audit policy subcategory s...	Not Defined
Audit: Shut down system immediately i...	Disabled
DCOM: Machine Access Restrictions in ...	Not Defined
DCOM: Machine Launch Restrictions in...	Not Defined
Devices: Allow undock without having ...	Enabled
Devices: Allowed to format and eject re...	Not Defined
Devices: Prevent users from installing p...	Enabled
Devices: Restrict CD-ROM access to loc...	Not Defined
Devices: Restrict floppy access to locall...	Not Defined
Domain controller: Allow server operat...	Not Defined
Domain controller: LDAP server signing...	Not Defined
Domain controller: Refuse machine acc...	Not Defined
Domain member: Digitally encrypt or si...	Enabled
Domain member: Digitally encrypt sec...	Enabled
Domain member: Digitally sign secure ...	Enabled

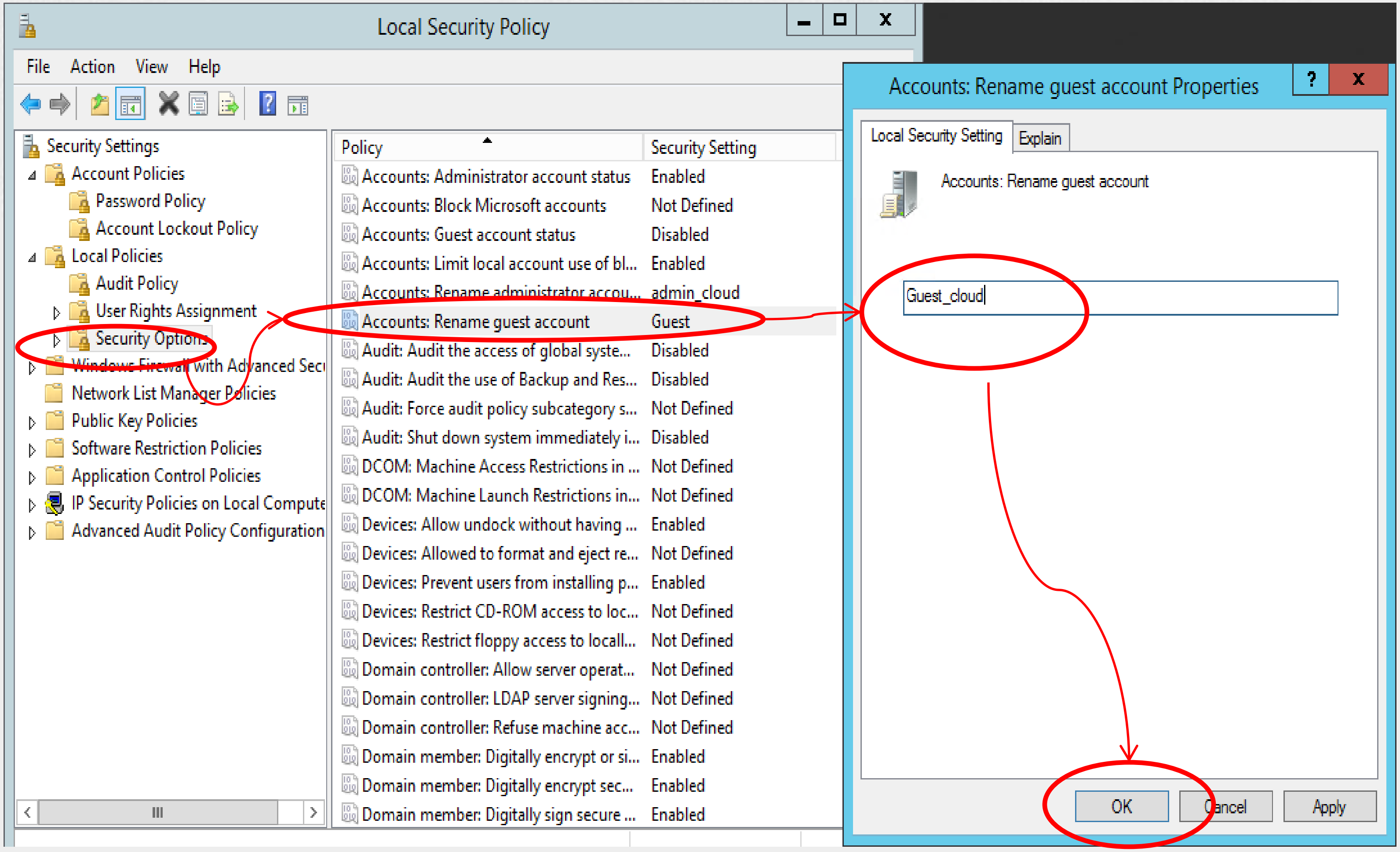
Accounts: Rename administrator account

admin_cloud

MS Windows Server 2012

Security Options

Configure 'Accounts: Rename Guest account'


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

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of bl...	Enabled
Accounts: Rename administrator accou...	admin_cloud
Accounts: Rename guest account	Guest
Audit: Audit the access of global syste...	Disabled
Audit: Audit the use of Backup and Res...	Disabled
Audit: Force audit policy subcategory s...	Not Defined
Audit: Shut down system immediately i...	Disabled
DCOM: Machine Access Restrictions in ...	Not Defined
DCOM: Machine Launch Restrictions in...	Not Defined
Devices: Allow undock without having ...	Enabled
Devices: Allowed to format and eject re...	Not Defined
Devices: Prevent users from installing p...	Enabled
Devices: Restrict CD-ROM access to loc...	Not Defined
Devices: Restrict floppy access to locall...	Not Defined
Domain controller: Allow server operat...	Not Defined
Domain controller: LDAP server signing...	Not Defined
Domain controller: Refuse machine acc...	Not Defined
Domain member: Digitally encrypt or si...	Enabled
Domain member: Digitally encrypt sec...	Enabled
Domain member: Digitally sign secure ...	Enabled

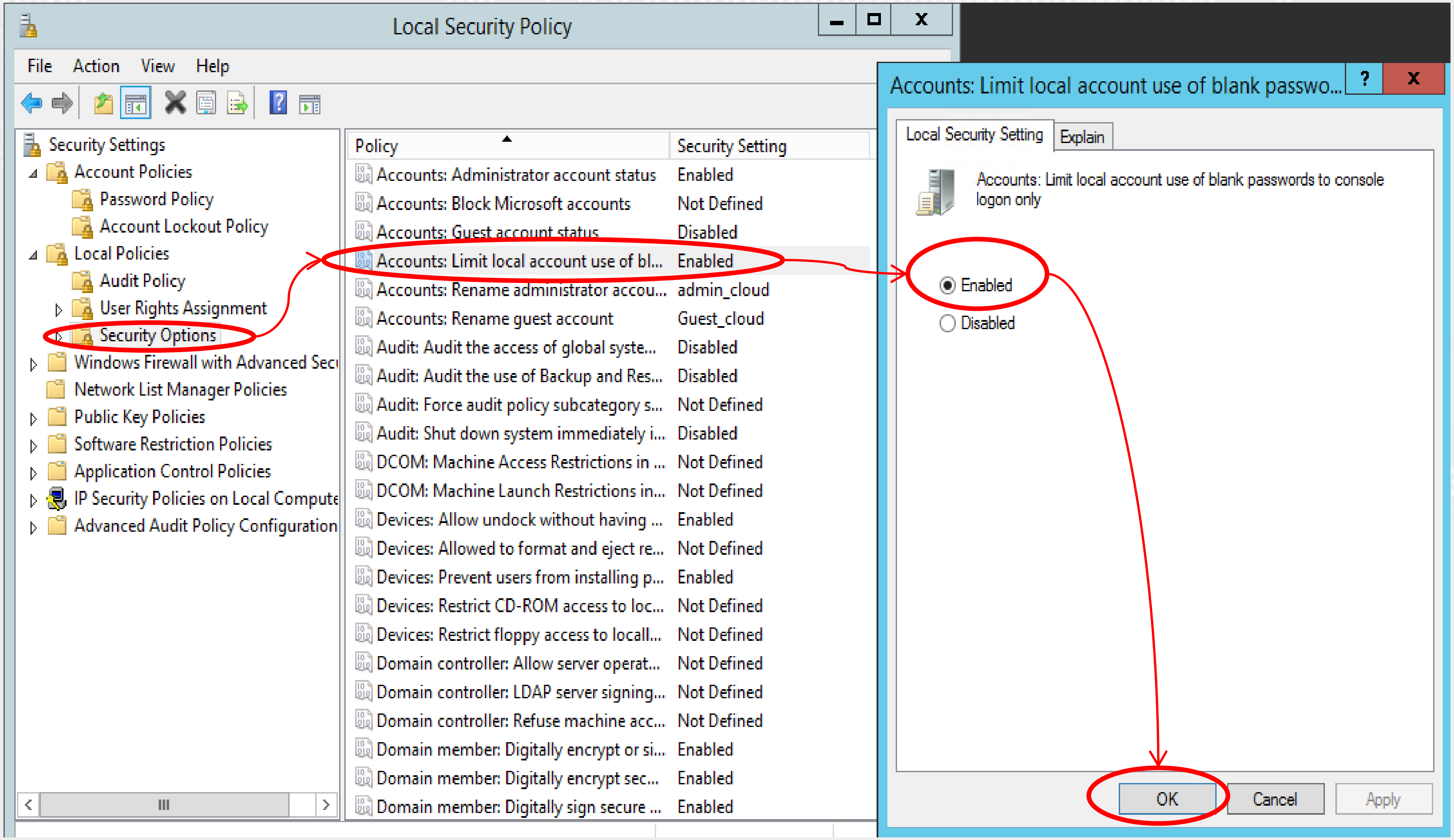
Accounts: Rename guest account

Guest_cloud

MS Windows Server 2012

Security Options

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



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

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of bl...	Enabled
Accounts: Rename administrator accou...	admin_cloud
Accounts: Rename guest account	Guest_cloud
Audit: Audit the access of global syste...	Disabled
Audit: Audit the use of Backup and Res...	Disabled
Audit: Force audit policy subcategory s...	Not Defined
Audit: Shut down system immediately i...	Disabled
DCOM: Machine Access Restrictions in ...	Not Defined
DCOM: Machine Launch Restrictions in...	Not Defined
Devices: Allow undock without having ...	Enabled
Devices: Allowed to format and eject re...	Not Defined
Devices: Prevent users from installing p...	Enabled
Devices: Restrict CD-ROM access to loc...	Not Defined
Devices: Restrict floppy access to locall...	Not Defined
Domain controller: Allow server operat...	Not Defined
Domain controller: LDAP server signing...	Not Defined
Domain controller: Refuse machine acc...	Not Defined
Domain member: Digitally encrypt or si...	Enabled
Domain member: Digitally encrypt sec...	Enabled
Domain member: Digitally sign secure ...	Enabled

Accounts: Limit local account use of blank passwo...

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

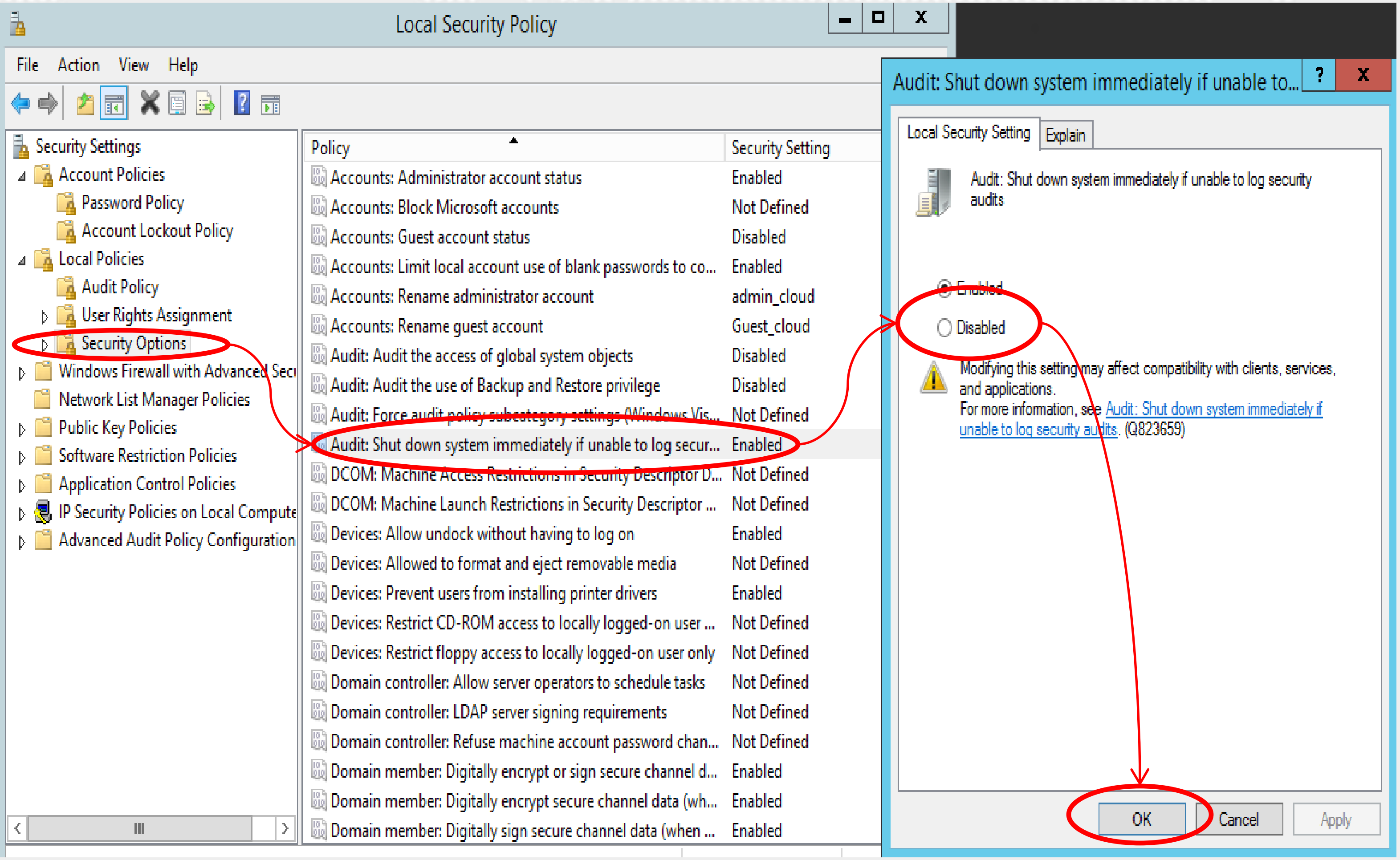
● Enabled

○ Disabled

MS Windows Server 2012

Security Options

Shut down system immediately if unable to log security audits



Local Security Policy

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

Policy	Security Setting
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
Audit: Shut down system immediately if unable to log secur...	Enabled
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...

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

● 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)

MS Windows Server 2012

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/

[illegible]

DEPARTMENT OF DEFENSE STANDARD

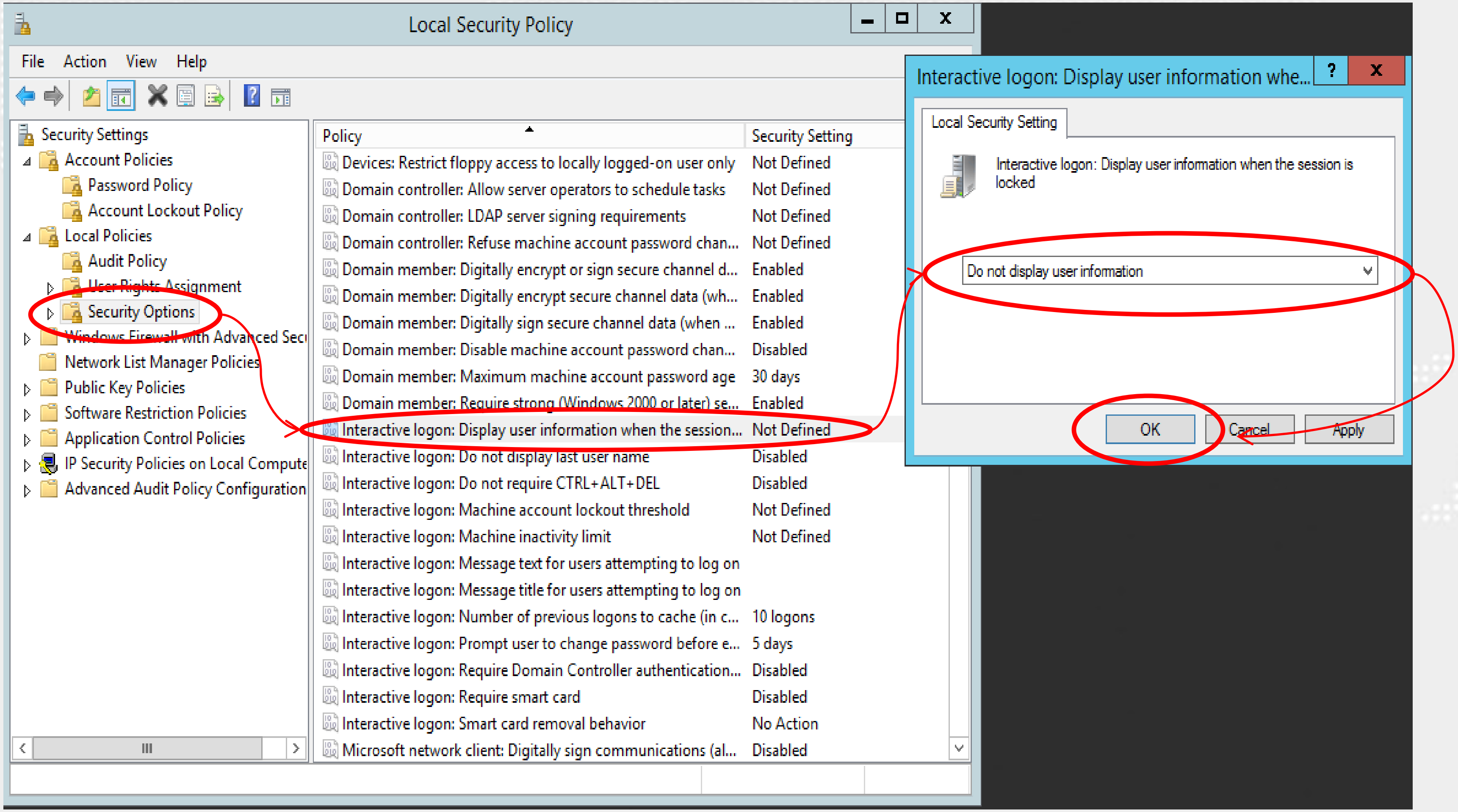
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

MS Windows Server 2012

Security Options

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



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

Policy	Security Setting
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...	Not Defined
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

Interactive logon: Display user information whe...

Local Security Setting

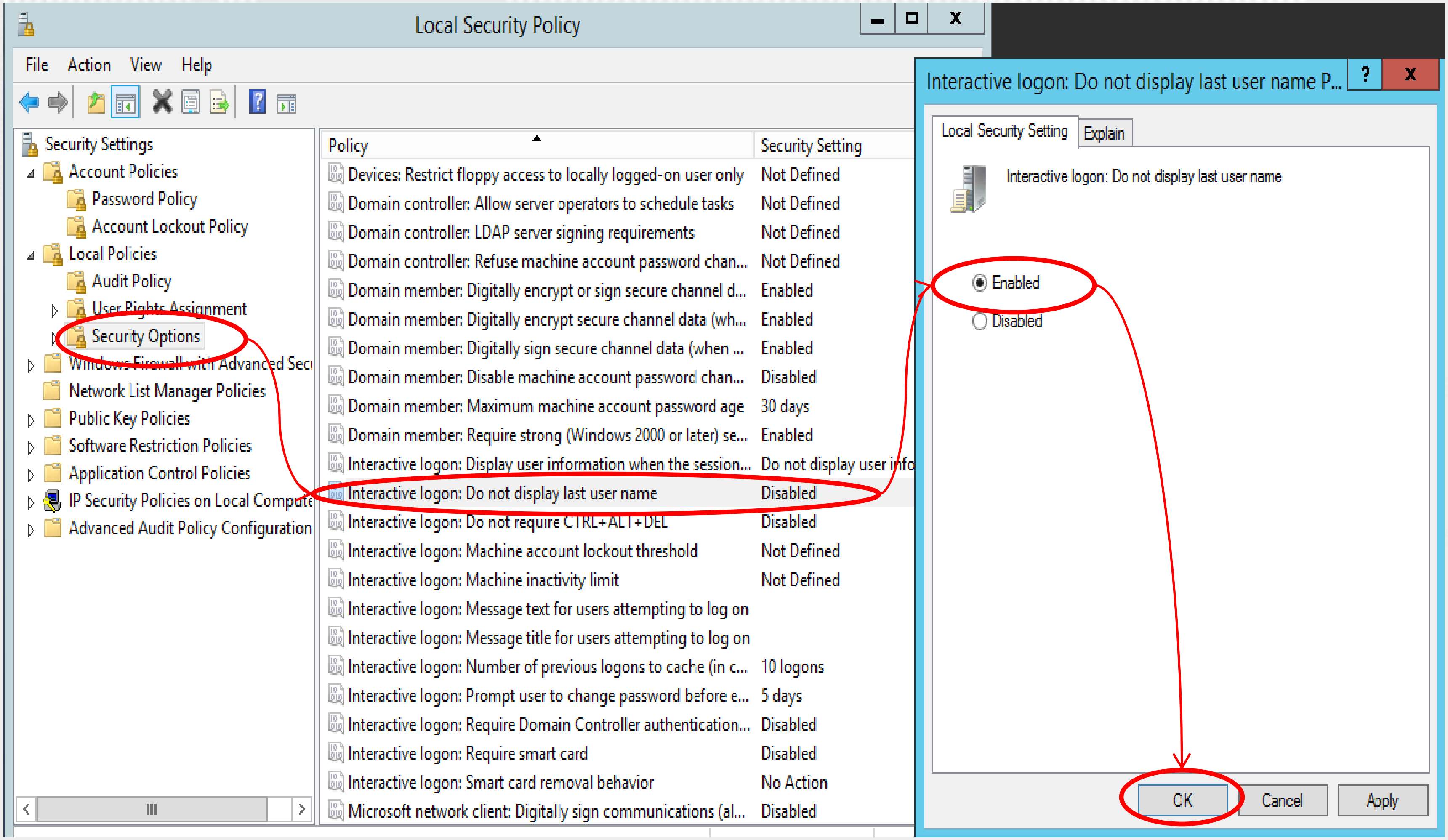
Interactive logon: Display user information when the session is locked

Do not display user information

MS Windows Server 2012

Security Options

Interactive logon: Do not display last user name



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

Policy	Security Setting
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	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

Interactive logon: Do not display last user name P...

Local Security Setting | Explain

Interactive logon: Do not display last user name

● Enabled

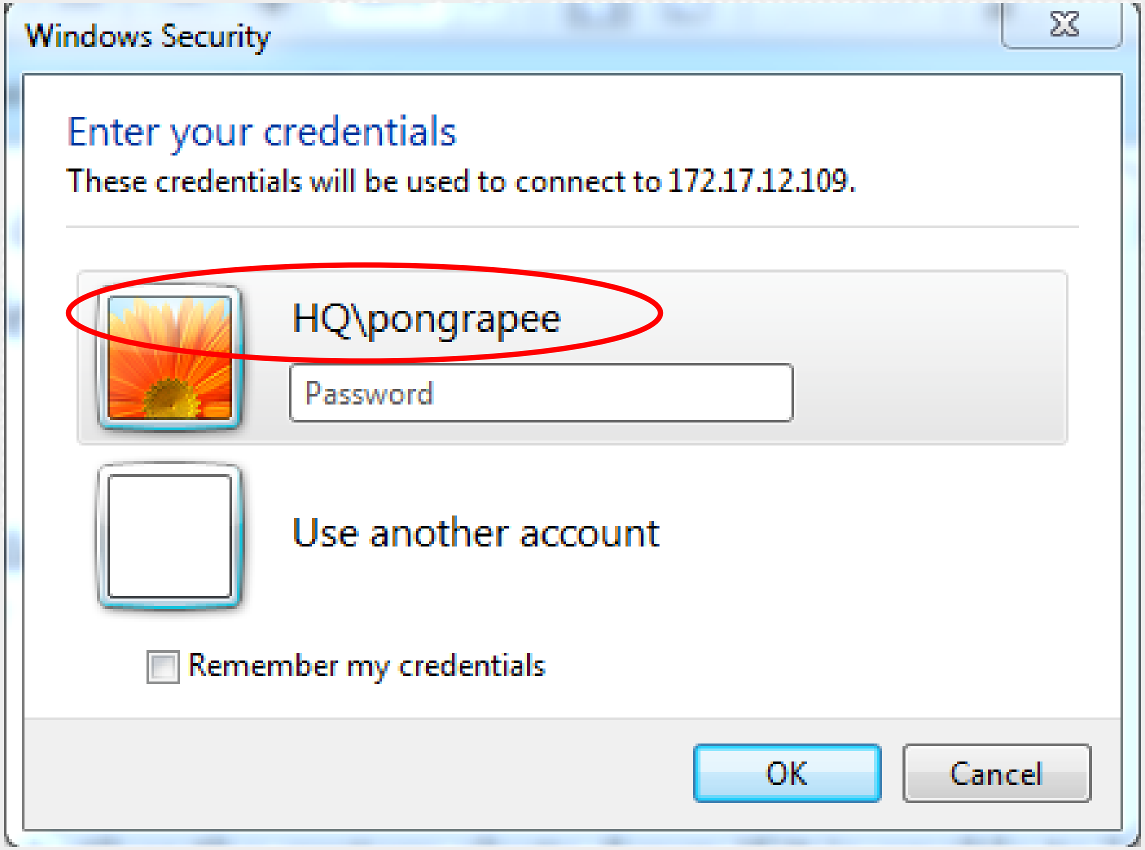
○ Disabled

OK Cancel Apply

MS Windows Server 2012

Security Options

Interactive logon: Do not display last user name



Windows Security

Enter your credentials

These credentials will be used to connect to 172.17.12.109.

HQ\pongrapee

Password

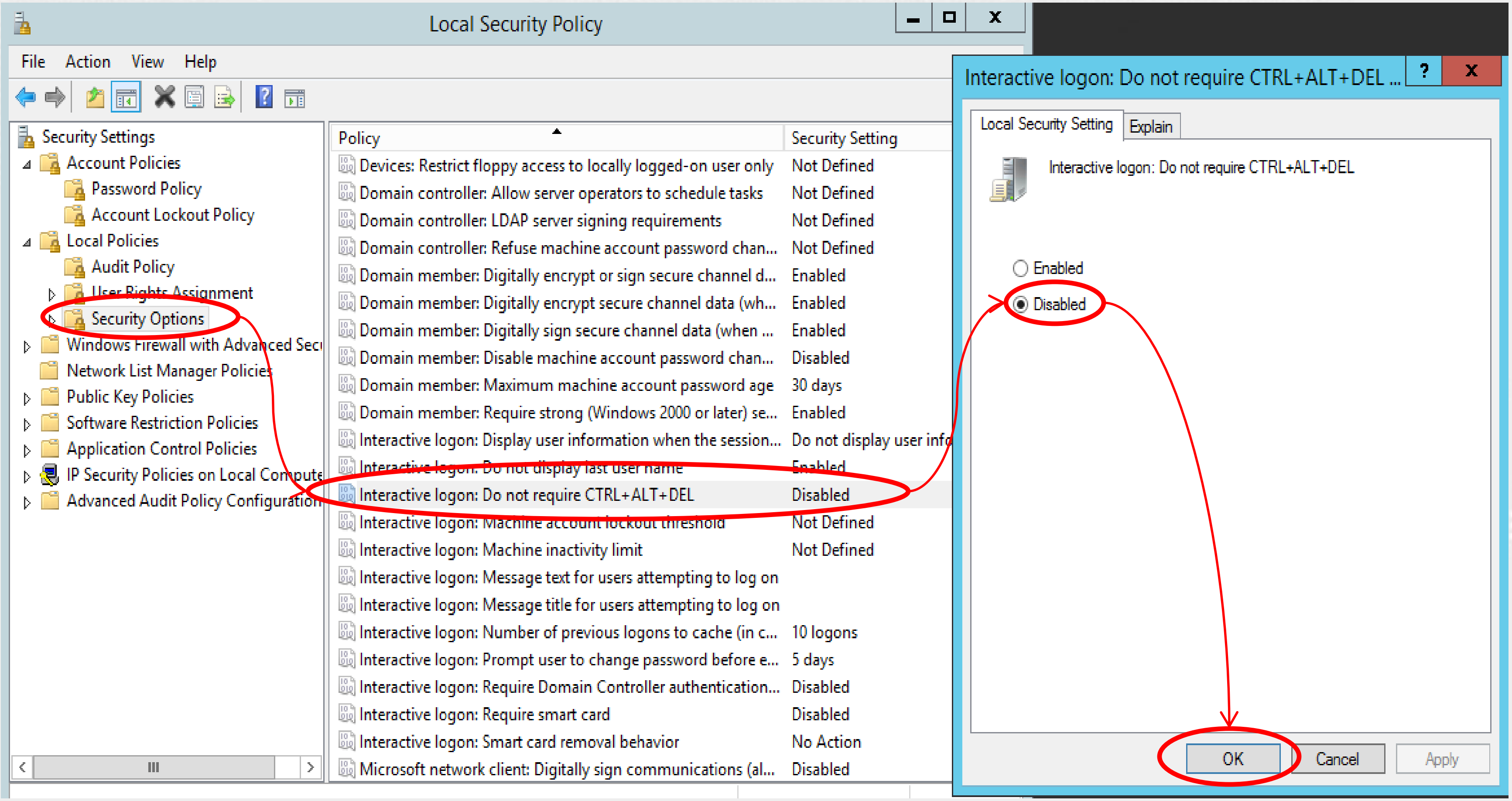
Use another account

□ Remember my credentials

MS Windows Server 2012

Security Options

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



Local Security Policy

File Action View Help

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

Policy	Security Setting
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

Interactive logon: Do not require CTRL+ALT+DEL ...

Local Security Setting | Explain

Interactive logon: Do not require CTRL+ALT+DEL

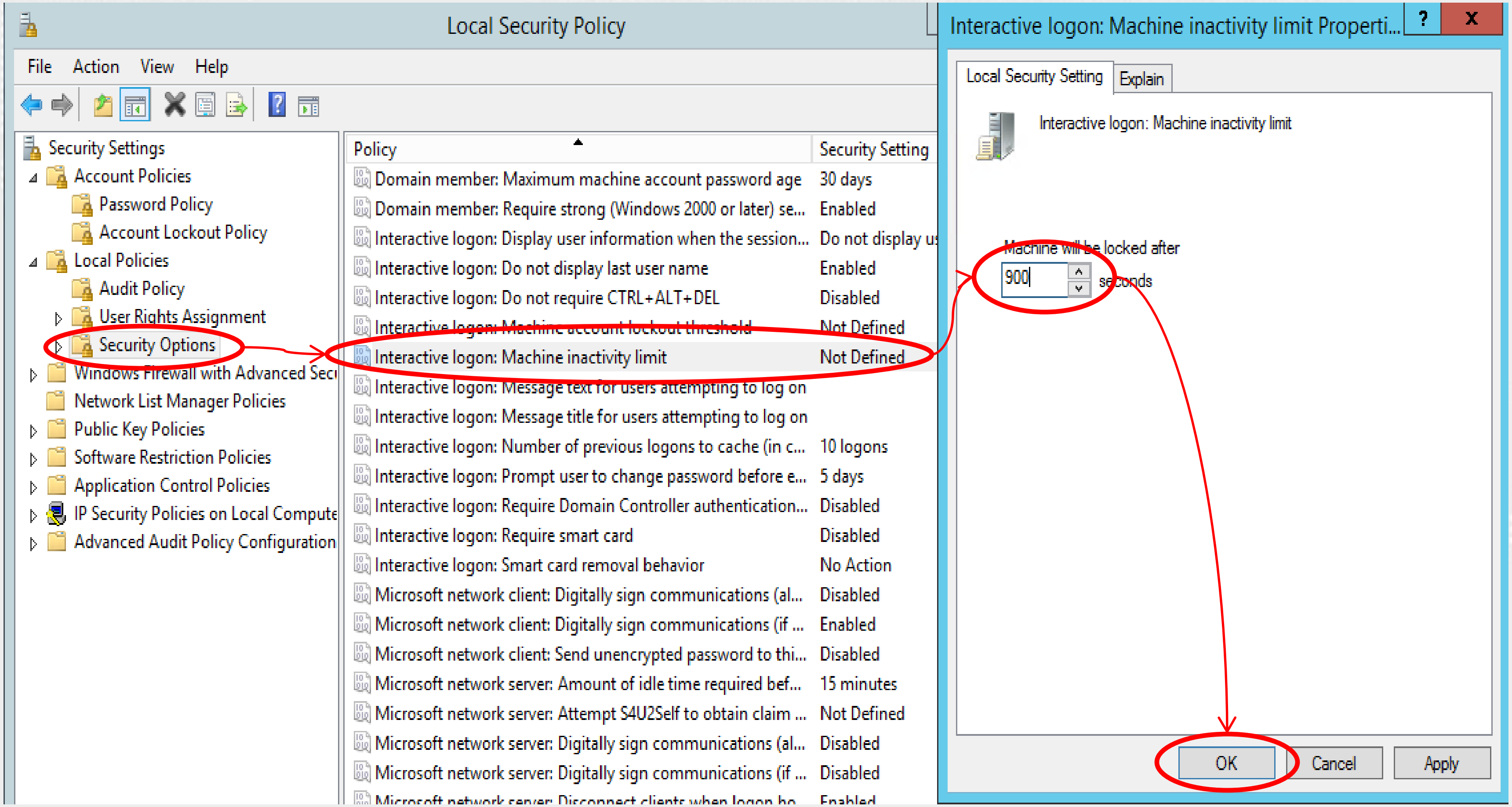
○ Enabled

● Disabled

MS Windows Server 2012

Security Options

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



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

Policy	Security Setting
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 ho...	Enabled

Interactive logon: Machine inactivity limit

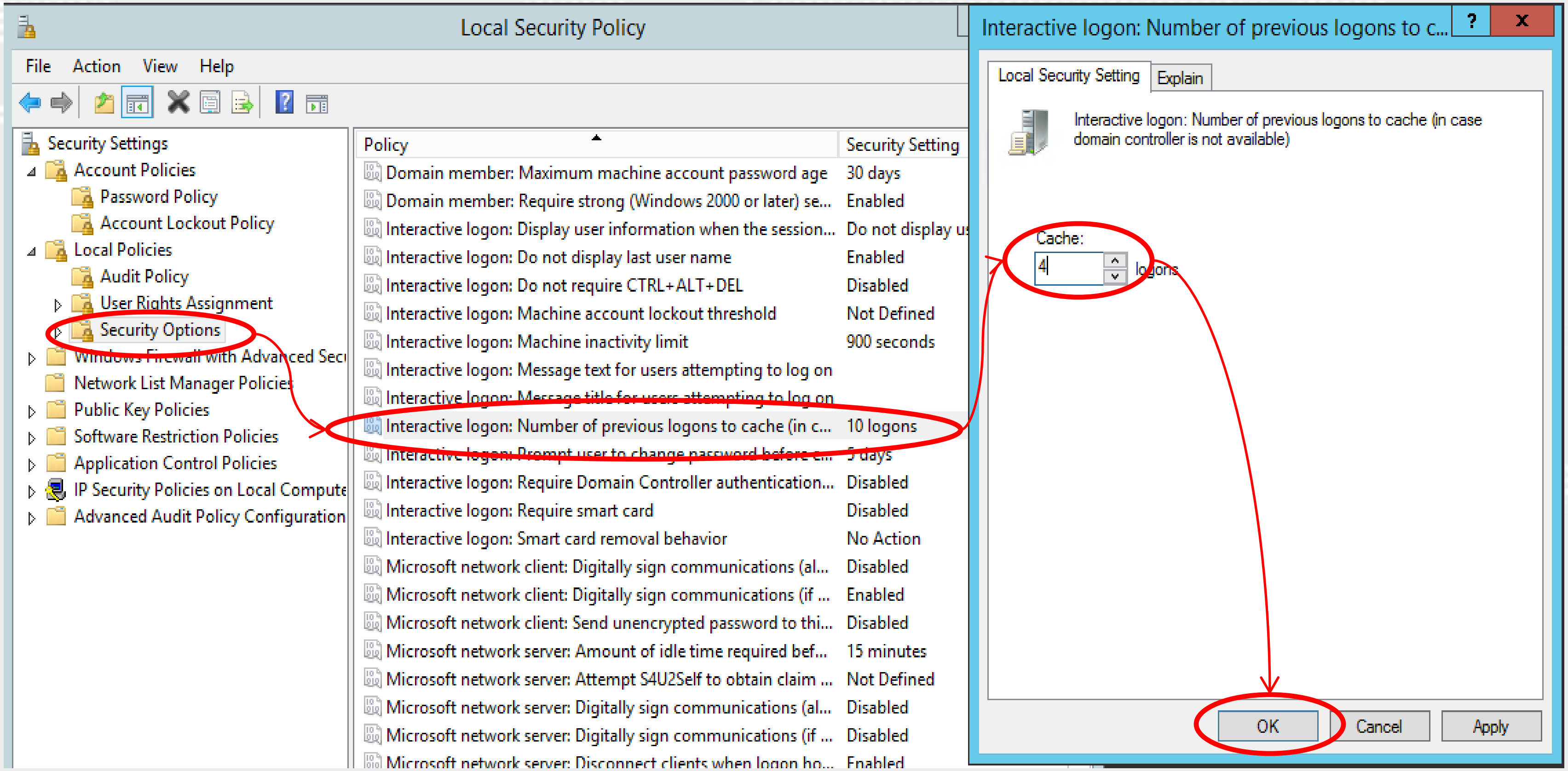
Machine will be locked after

900 seconds

MS Windows Server 2012

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

Policy	Security Setting
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...	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 ho...	Enabled

Interactive logon: Number of previous logons to c...

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

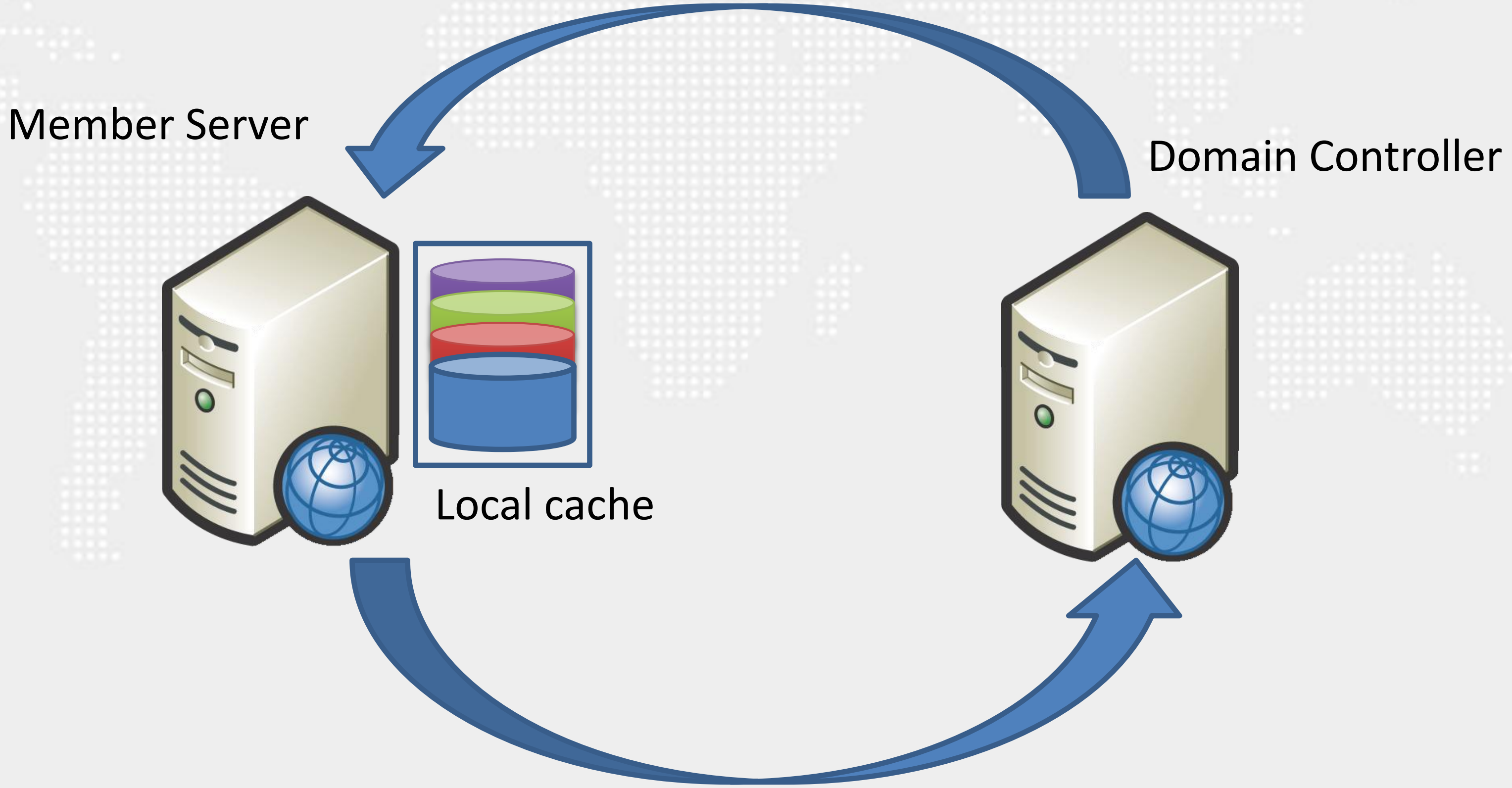
Cache:

4 logons

MS Windows Server 2012

Security Options

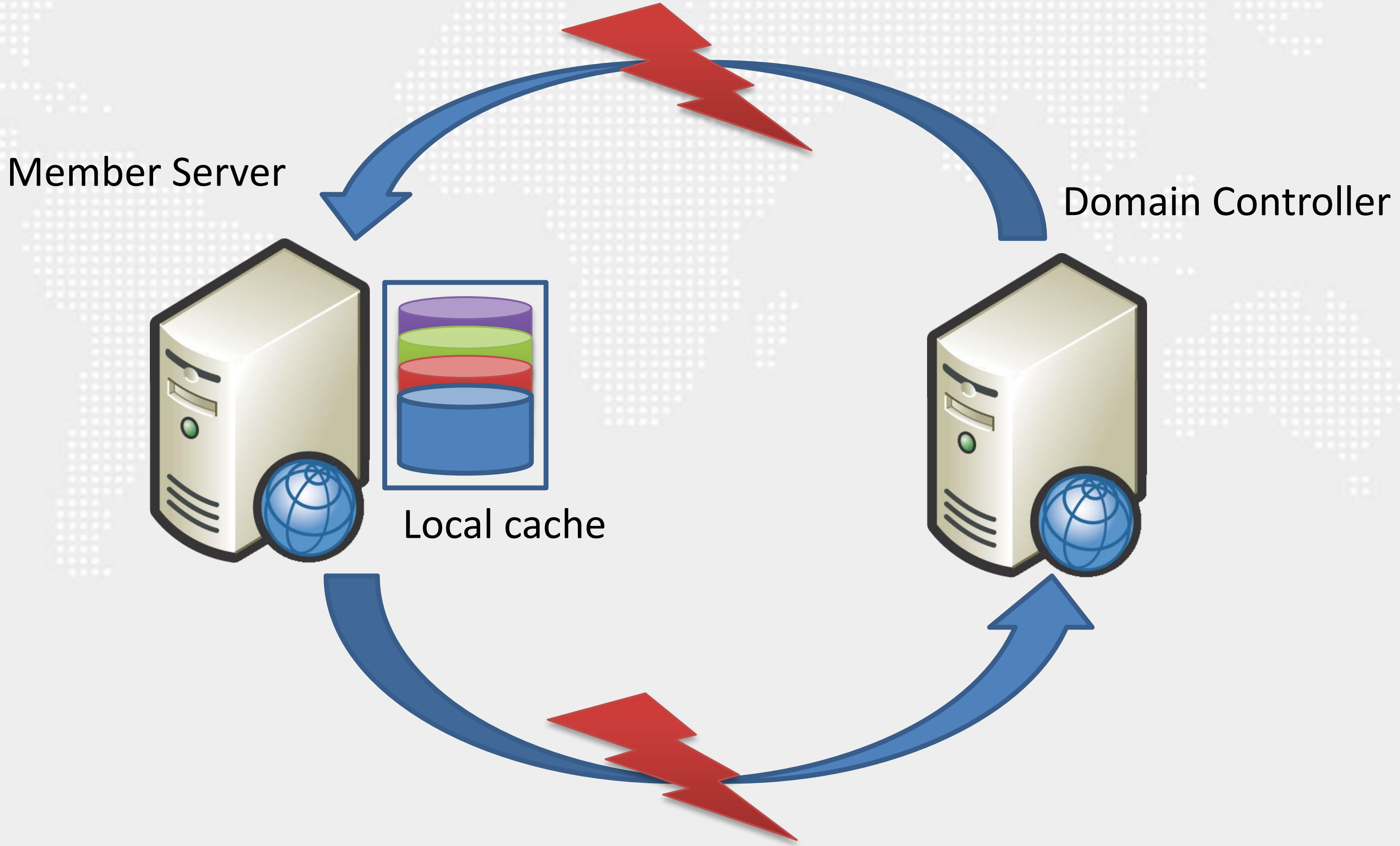
Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



MS Windows Server 2012

Security Options

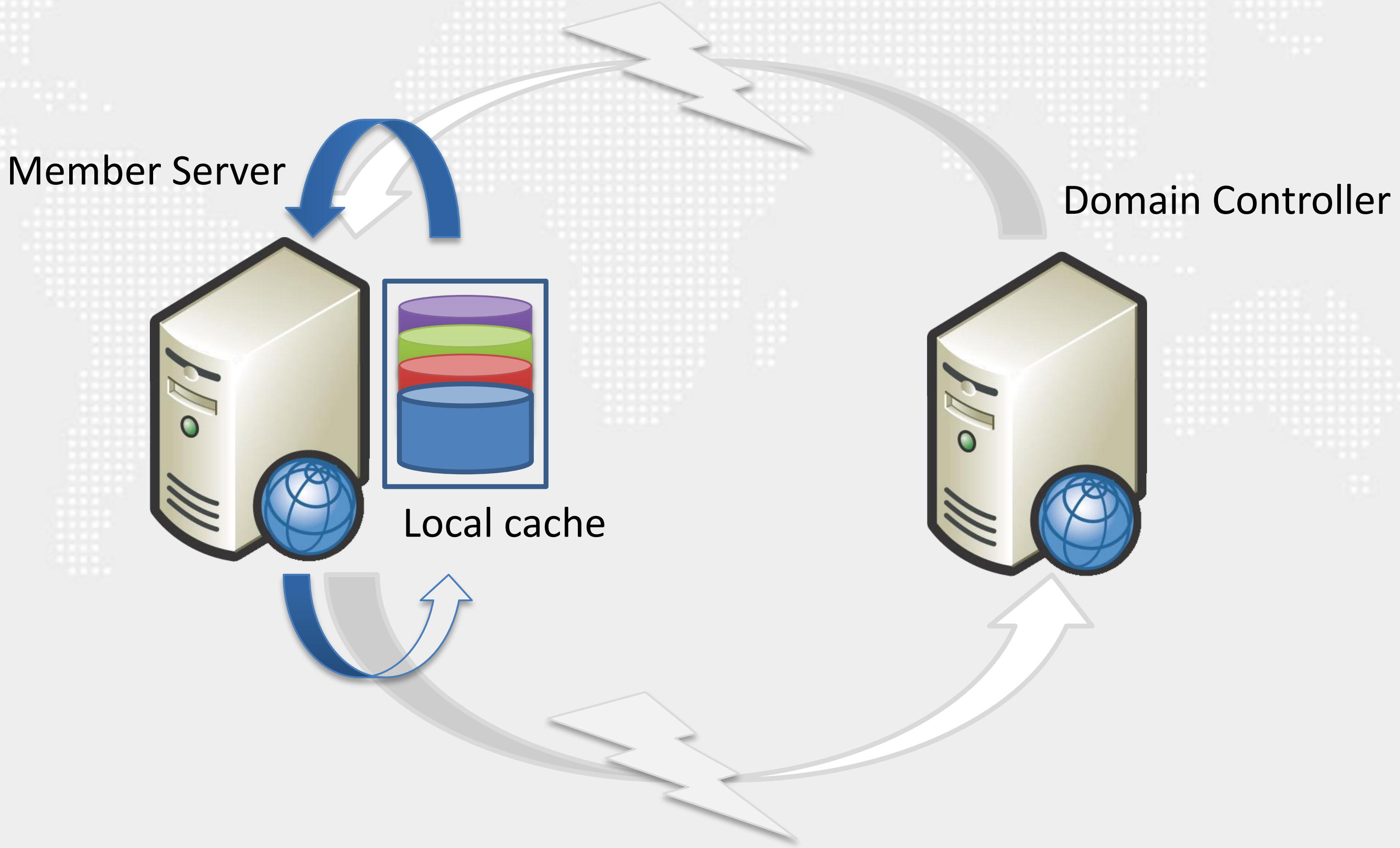
Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



MS Windows Server 2012

Security Options

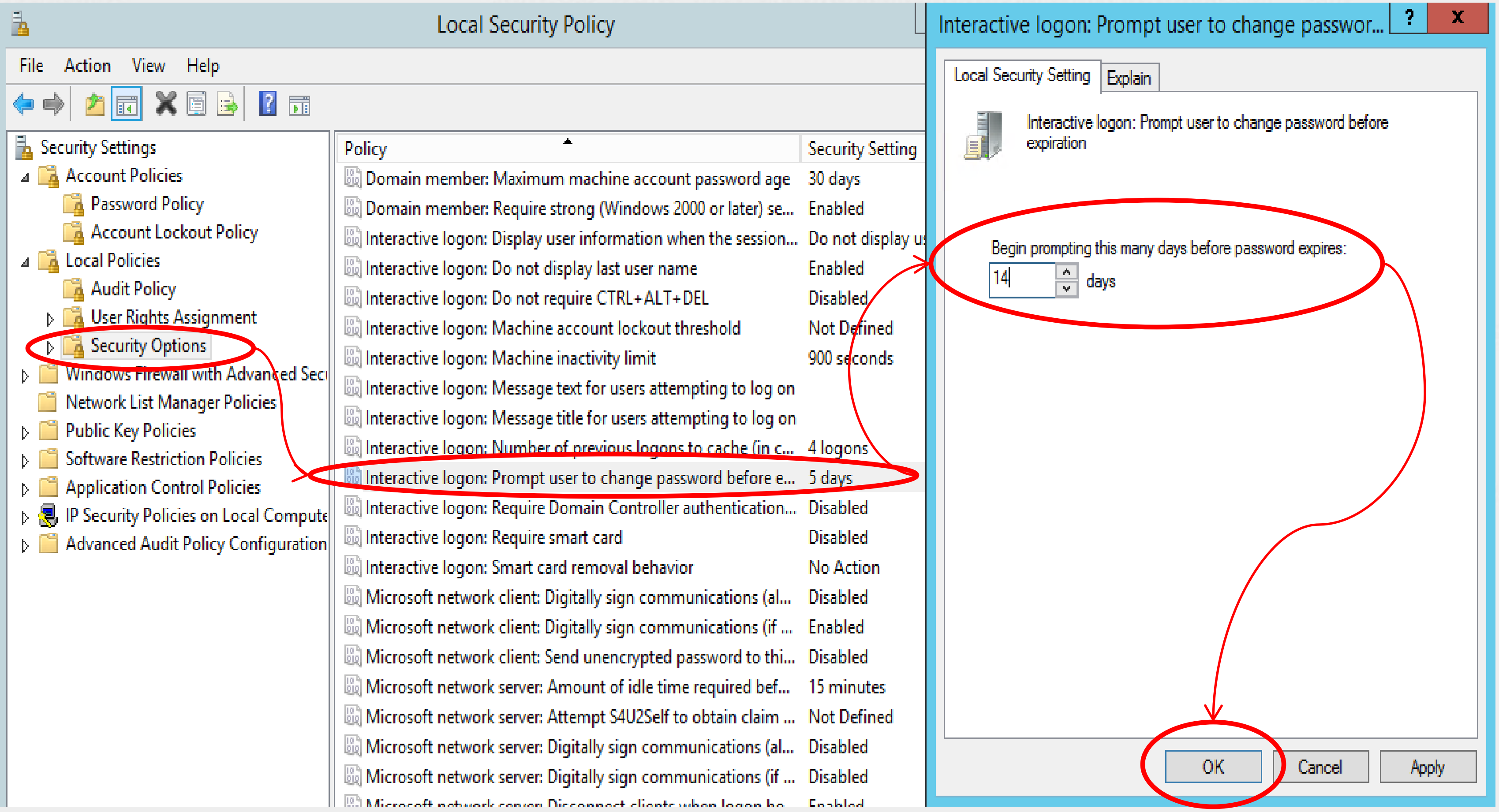
Set 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' to '4 or fewer logon(s)'



MS Windows Server 2012

Security Options

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



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 logon ho...	Enabled

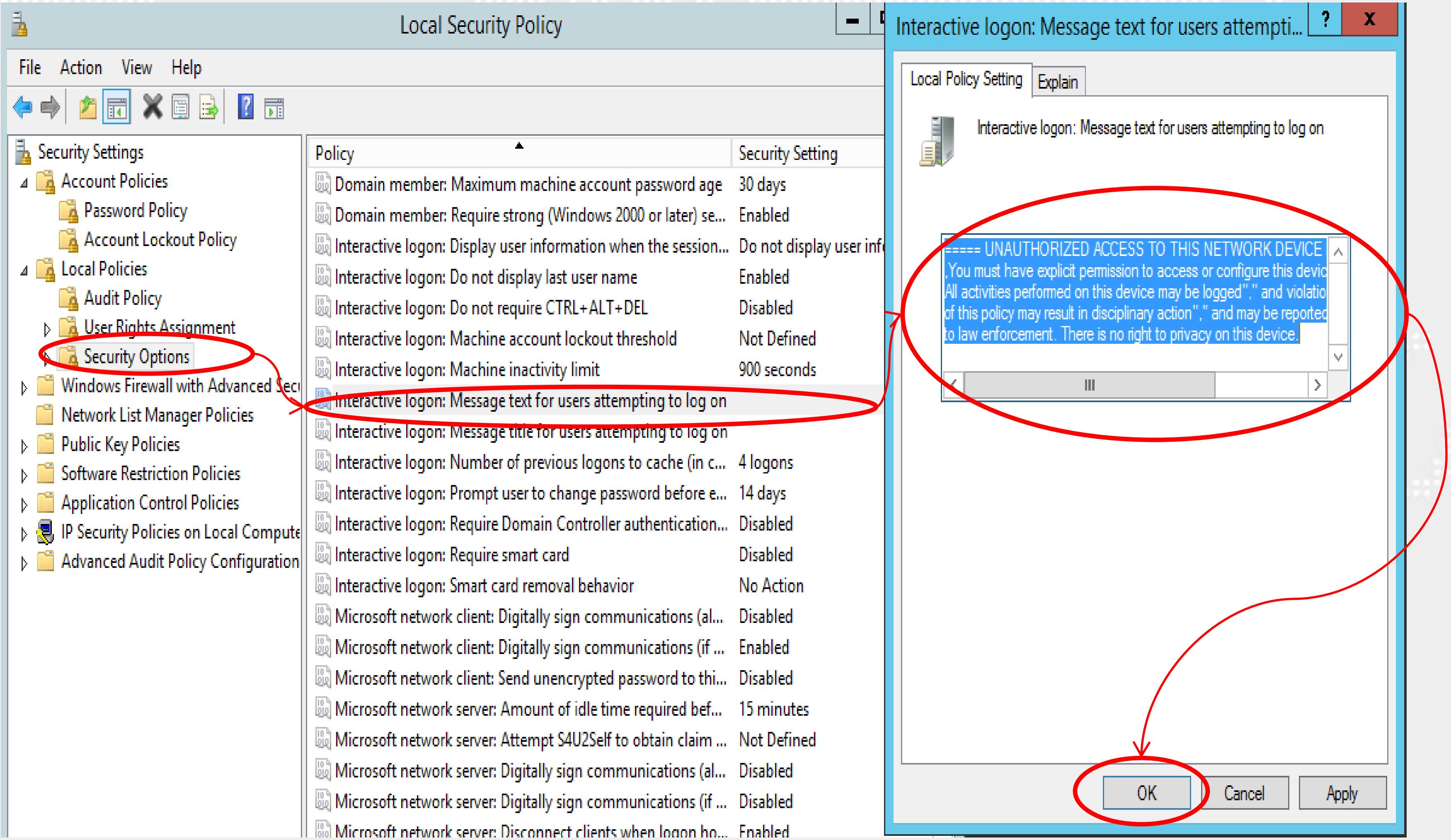
Interactive logon: Prompt user to change password before expiration

Begin prompting this many days before password expires: 14 days

MS Windows Server 2012

Security Options

Interactive logon: Message text for users attempting to log on



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

Policy	Security Setting
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	
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 logon ho...	Enabled

Interactive logon: Message text for users attempting to log on

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

MS Windows Server 2012

Security Options

Interactive logon: Message text for users attempting to log on

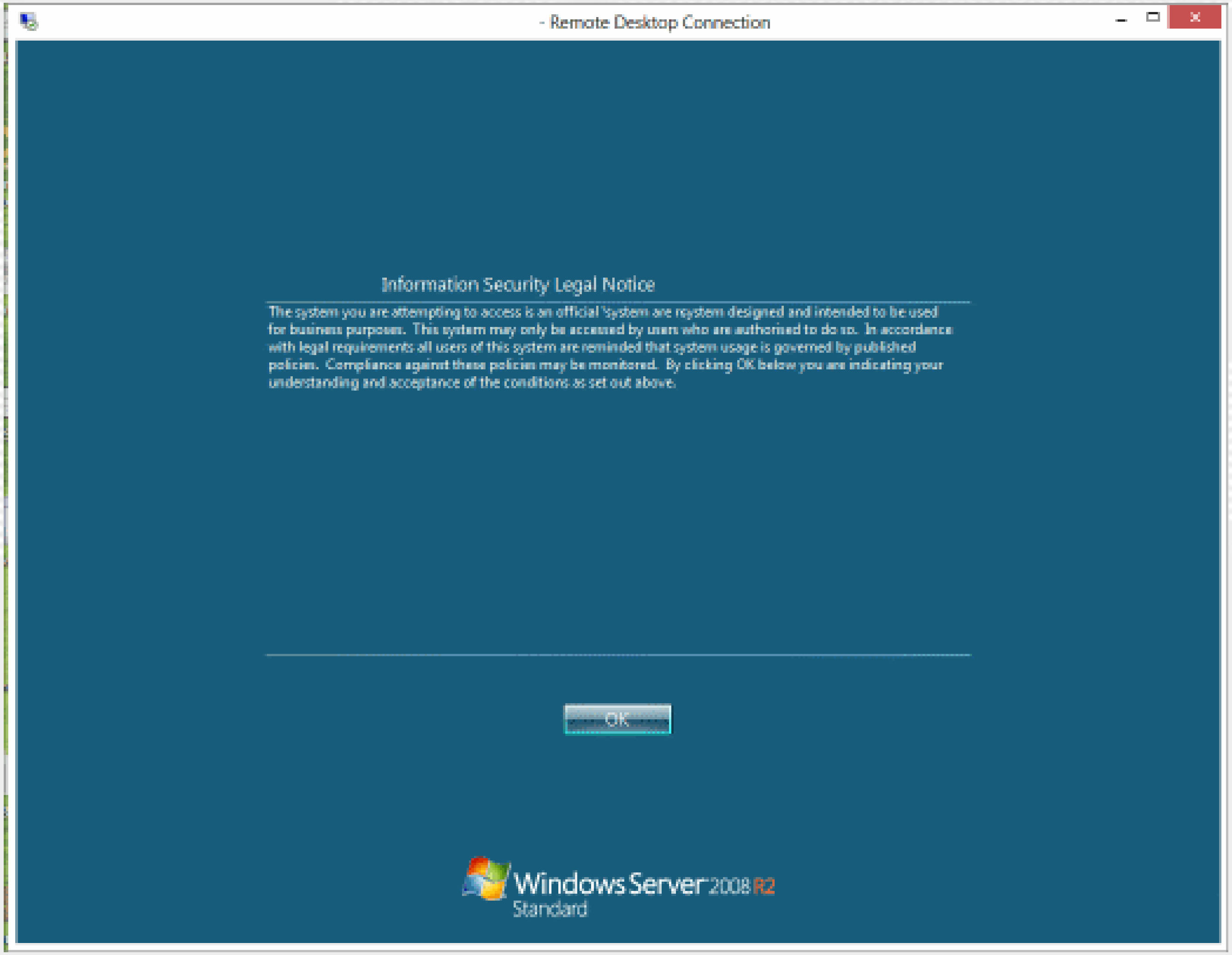
===== UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. =====
,You must have explicit permission to access or configure this device.,
“All activities performed on this device may be logged"," and violations,
of this policy may result in disciplinary action"," and may be reported,
to law enforcement.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

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

MS Windows Server 2012

Security Options

Interactive logon: Message text for users attempting to log on



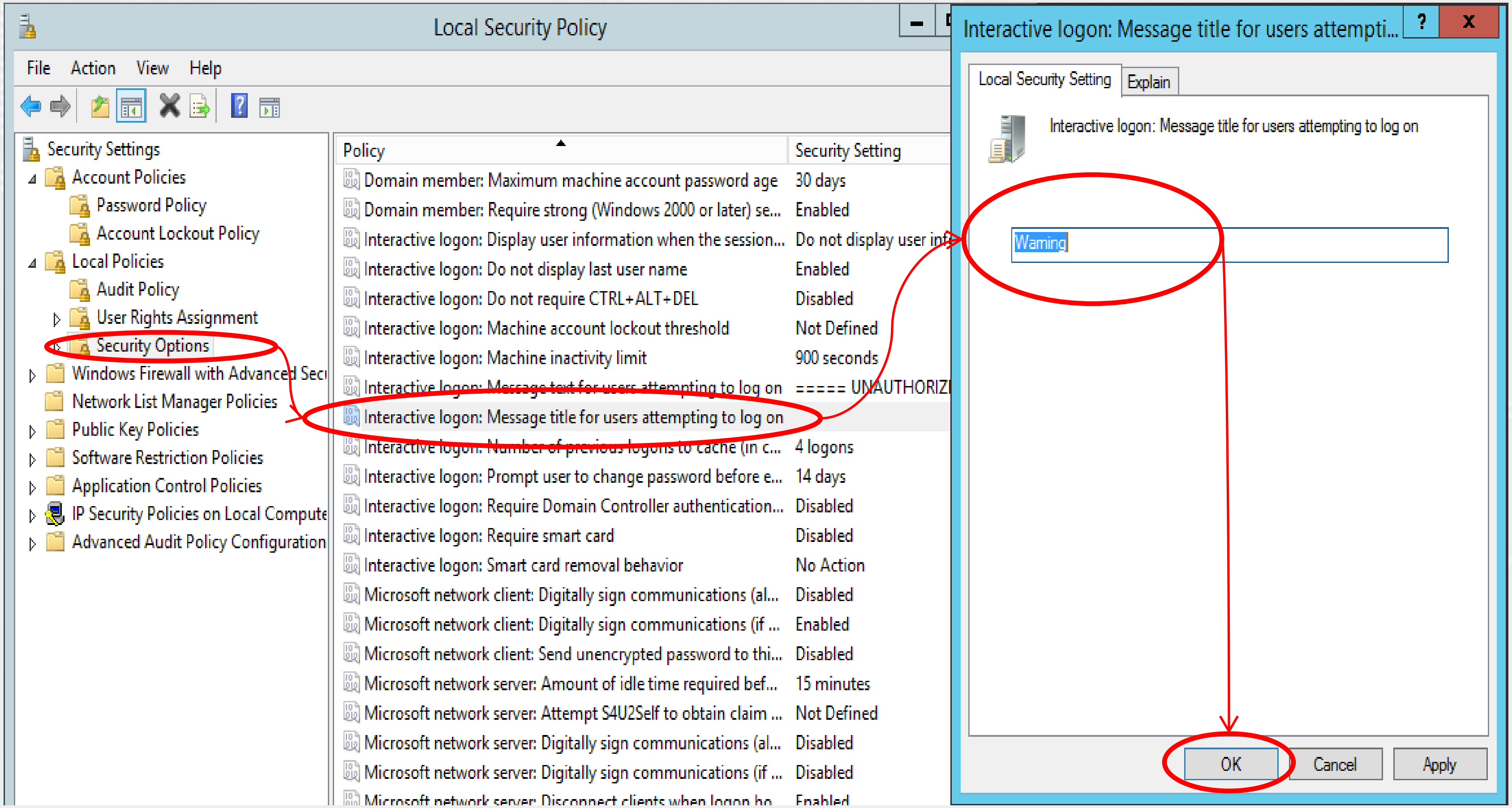
Information Security Legal Notice

The system you are attempting to access is an official 'System are rsystem designed and intended to be used for business purposes. This system may only be accessed by users who are authorised to do so. In accordance with legal requirements all users of this system are reminded that system usage is governed by published policies. Compliance against these policies may be monitored. By clicking OK below you are indicating your understanding and acceptance of the conditions as set out above.

MS Windows Server 2012

Security Options

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



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

Policy	Security Setting
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	===== UNAUTHORIZI
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 logon ho...	Enabled

Interactive logon: Message title for users attempting to log on

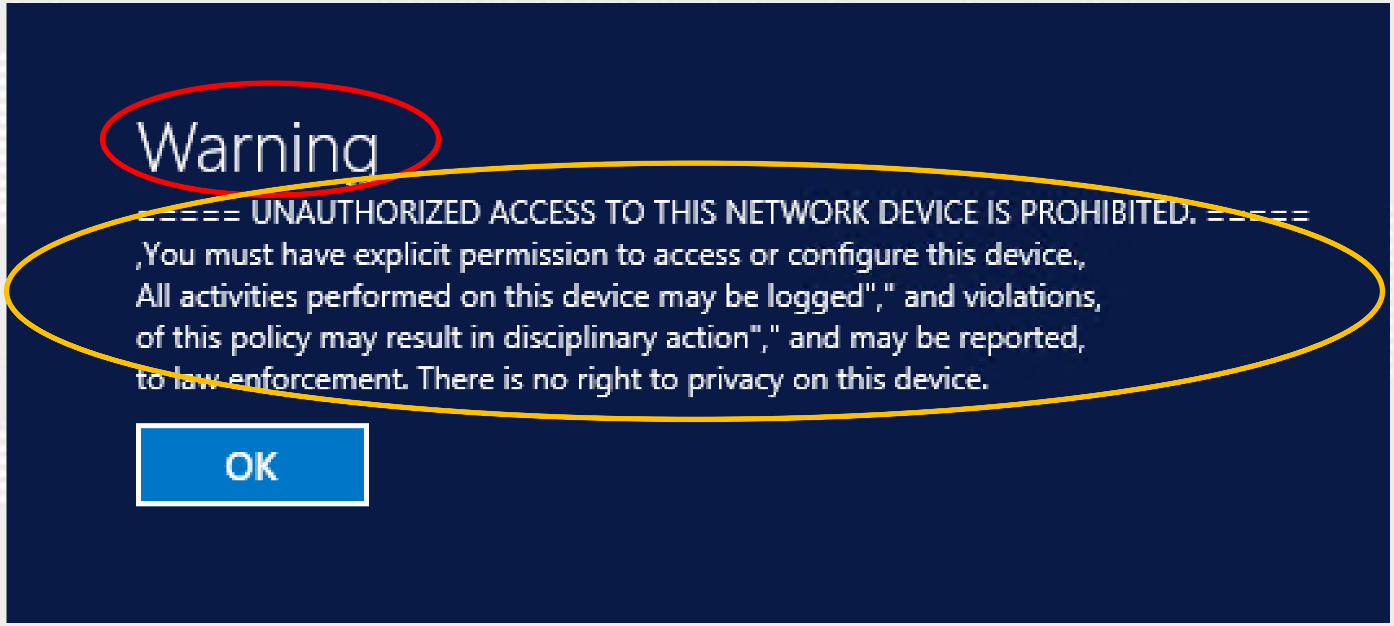
Warning

MS Windows Server 2012

Security Options

Interactive logon: Message text for users attempting to log on

Interactive logon: Message title for users attempting to log on



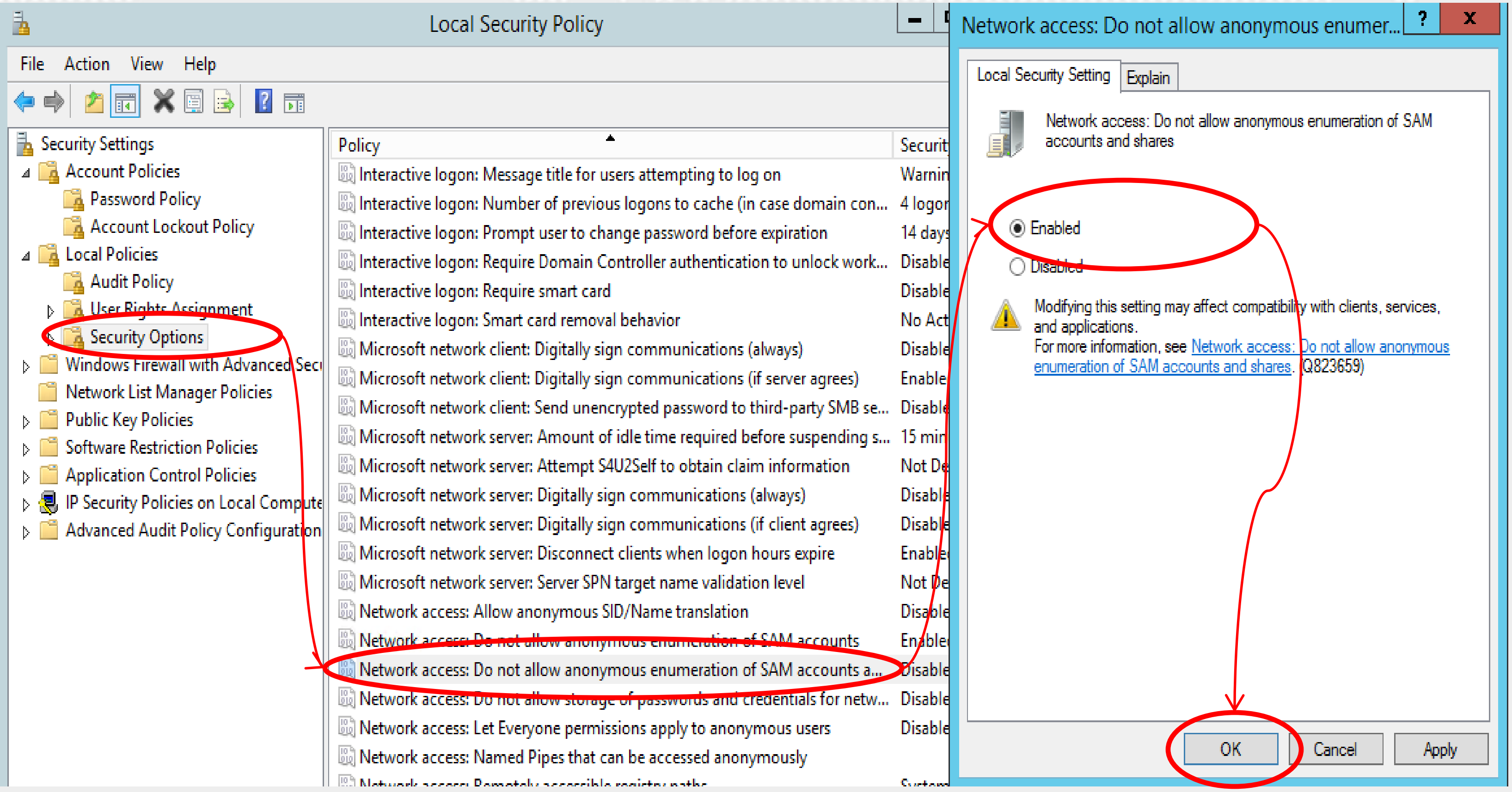
Warning

===== 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.

MS Windows Server 2012

Security Options

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



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

Policy	Securit
Interactive logon: Message title for users attempting to log on	Warnin
Interactive logon: Number of previous logons to cache (in case domain con...	4 logor
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock work...	Disable
Interactive logon: Require smart card	Disable
Interactive logon: Smart card removal behavior	No Act
Microsoft network client: Digitally sign communications (always)	Disable
Microsoft network client: Digitally sign communications (if server agrees)	Enable
Microsoft network client: Send unencrypted password to third-party SMB se...	Disable
Microsoft network server: Amount of idle time required before suspending s...	15 min
Microsoft network server: Attempt S4U2Self to obtain claim information	Not De
Microsoft network server: Digitally sign communications (always)	Disable
Microsoft network server: Digitally sign communications (if client agrees)	Disable
Microsoft network server: Disconnect clients when logon hours expire	Enable
Microsoft network server: Server SPN target name validation level	Not De
Network access: Allow anonymous SID/Name translation	Disable
Network access: Do not allow anonymous enumeration of SAM accounts	Enable
Network access: Do not allow anonymous enumeration of SAM accounts a...	Disable
Network access: Do not allow storage of passwords and credentials for netw...	Disable
Network access: Let Everyone permissions apply to anonymous users	Disable
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System

Network access: Do not allow anonymous enumer...

Network access: Do not allow anonymous enumeration of SAM accounts and shares

● Enabled

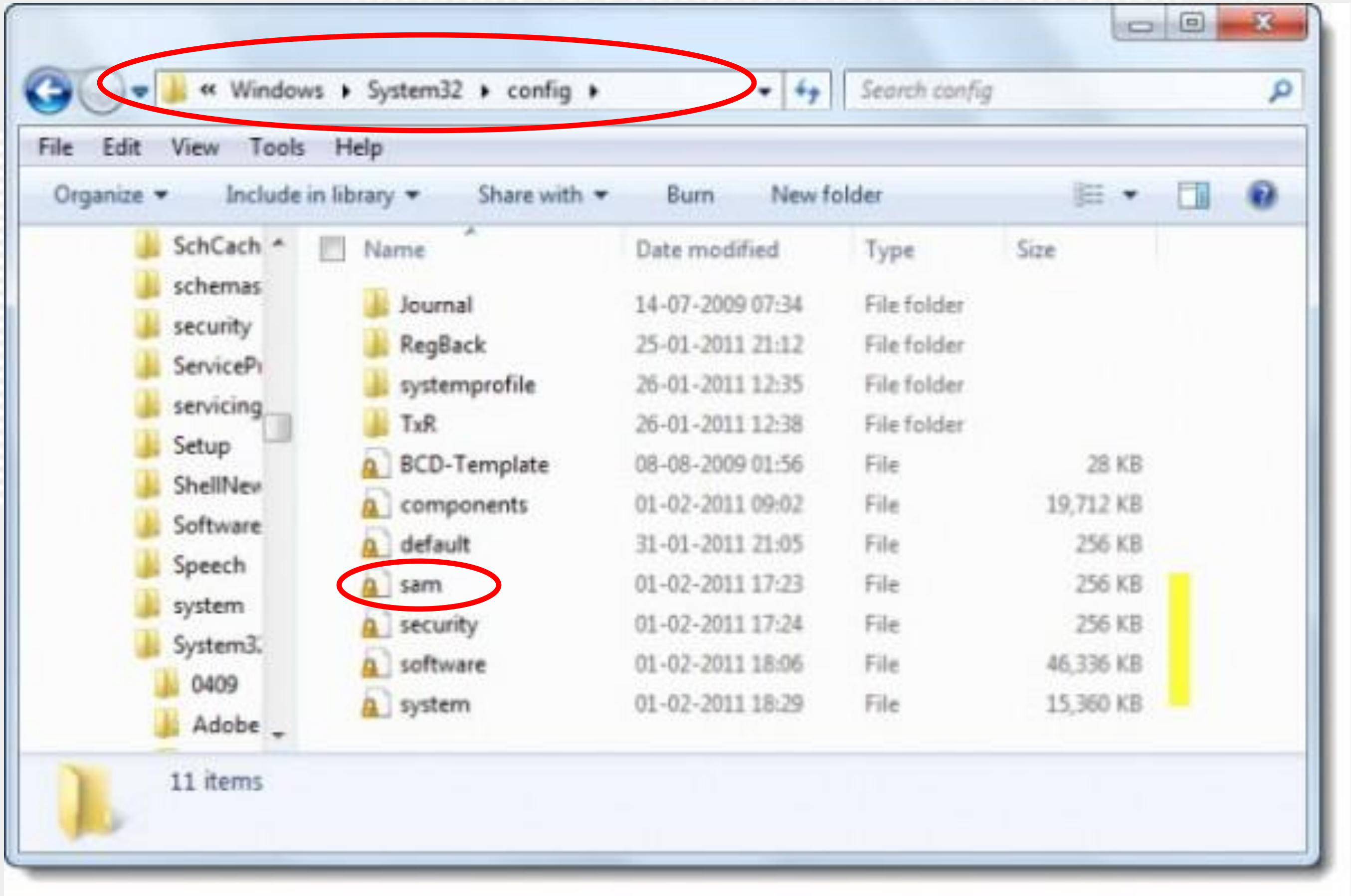
○ Disabled

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network access: Do not allow anonymous enumeration of SAM accounts and shares. (Q823659)

MS Windows Server 2012

Security Options

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



« Windows ▸ System32 ▸ config ▸
Search config
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ Burn New folder
SchCach
schemas
security
ServiceP
servicing
Setup
ShellNew
Software
Speech
system
System3
0409
Adobe
11 items

Name	Date modified	Type	Size
Journal	14-07-2009 07:34	File folder	
RegBack	25-01-2011 21:12	File folder	
systemprofile	26-01-2011 12:35	File folder	
TxR	26-01-2011 12:38	File folder	
BCD-Template	08-08-2009 01:56	File	28 KB
components	01-02-2011 09:02	File	19,712 KB
default	31-01-2011 21:05	File	256 KB
sam	01-02-2011 17:23	File	256 KB
security	01-02-2011 17:24	File	256 KB
software	01-02-2011 18:06	File	46,336 KB
system	01-02-2011 18:29	File	15,360 KB

MS Windows Server 2012

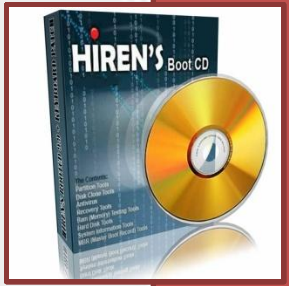
Security Options

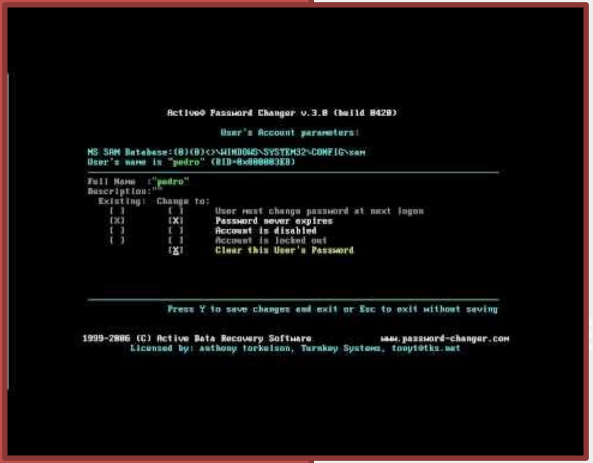
Set 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' to 'Enabled'

MS Windows Server 2012

Security Options

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



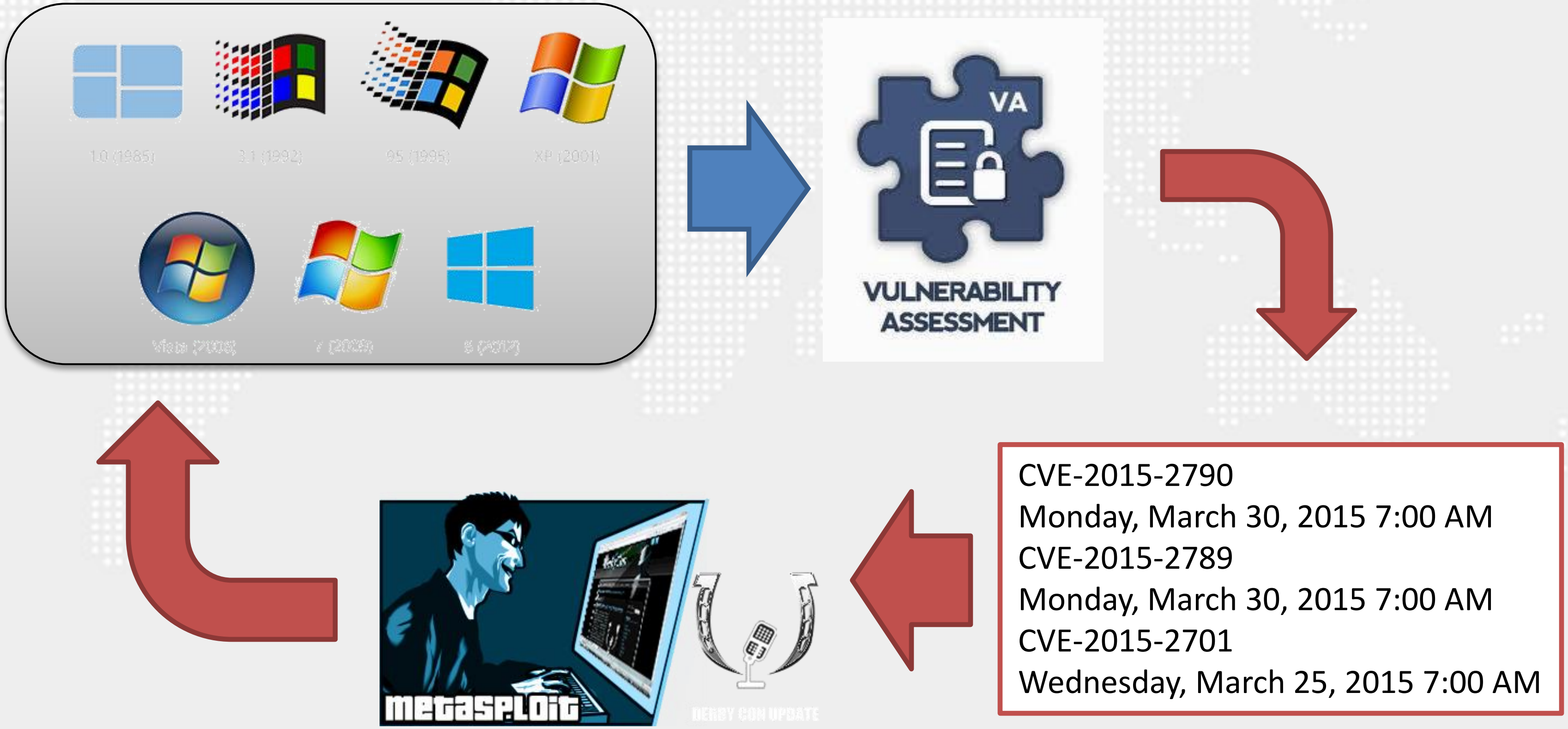


```
                Active@ Password Changer v.3.0 (build 0420)

                         User's Account parameters:

MS SAM Database:(0)(0)<>\WINDOWS\SYSTEM32\CONFIG\sam
User's name is "pedro" (RID=0x000003E8)
___________________________________________________________________
Full Name  :"pedro"
Description:""
  Existing:  Change to:
    [ ]        [ ]       User must change password at next logon
    [X]        [X]       Password never expires
    [ ]        [ ]       Account is disabled
    [ ]        [ ]       Account is locked out
               [X]       Clear this User's Password

___________________________________________________________________
               Press Y to save changes and exit or Esc to exit without saving

1999-2006 (C) Active Data Recovery Software            www.password-changer.com
    Licensed by: anthony torkelson, Turnkey Systems, tonyt@tks.net
```

MS Windows Server 2012

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/

MS Windows Server 2012

Security Options

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

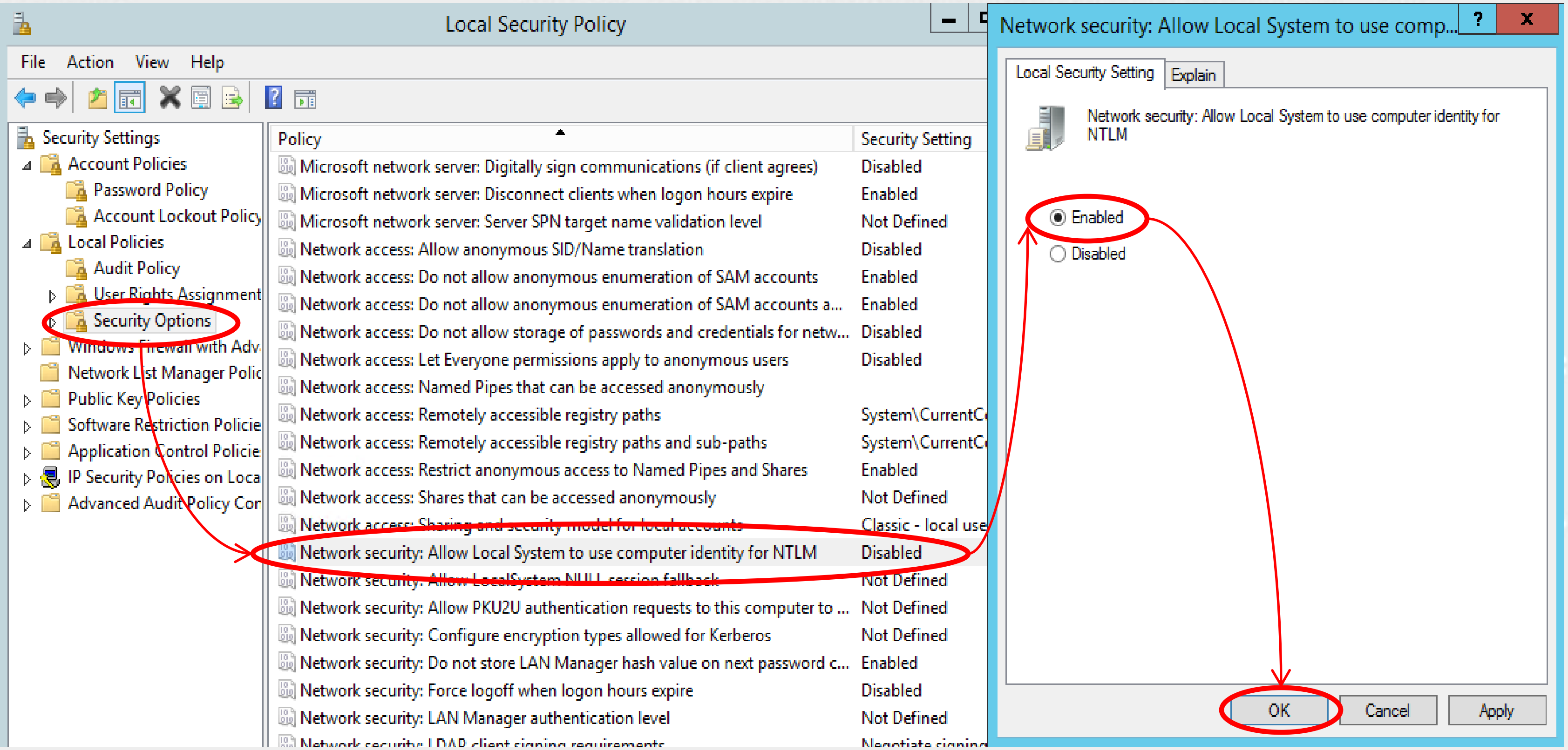
SAM

HIREN'S Boot CD

MS Windows Server 2012

Security Options

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



Policy	Security Setting
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts a...	Enabled
Network access: Do not allow storage of passwords and credentials for netw...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
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	Disabled
Network security: Allow LocalSystem NULL session fallback	Not Defined
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
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing

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

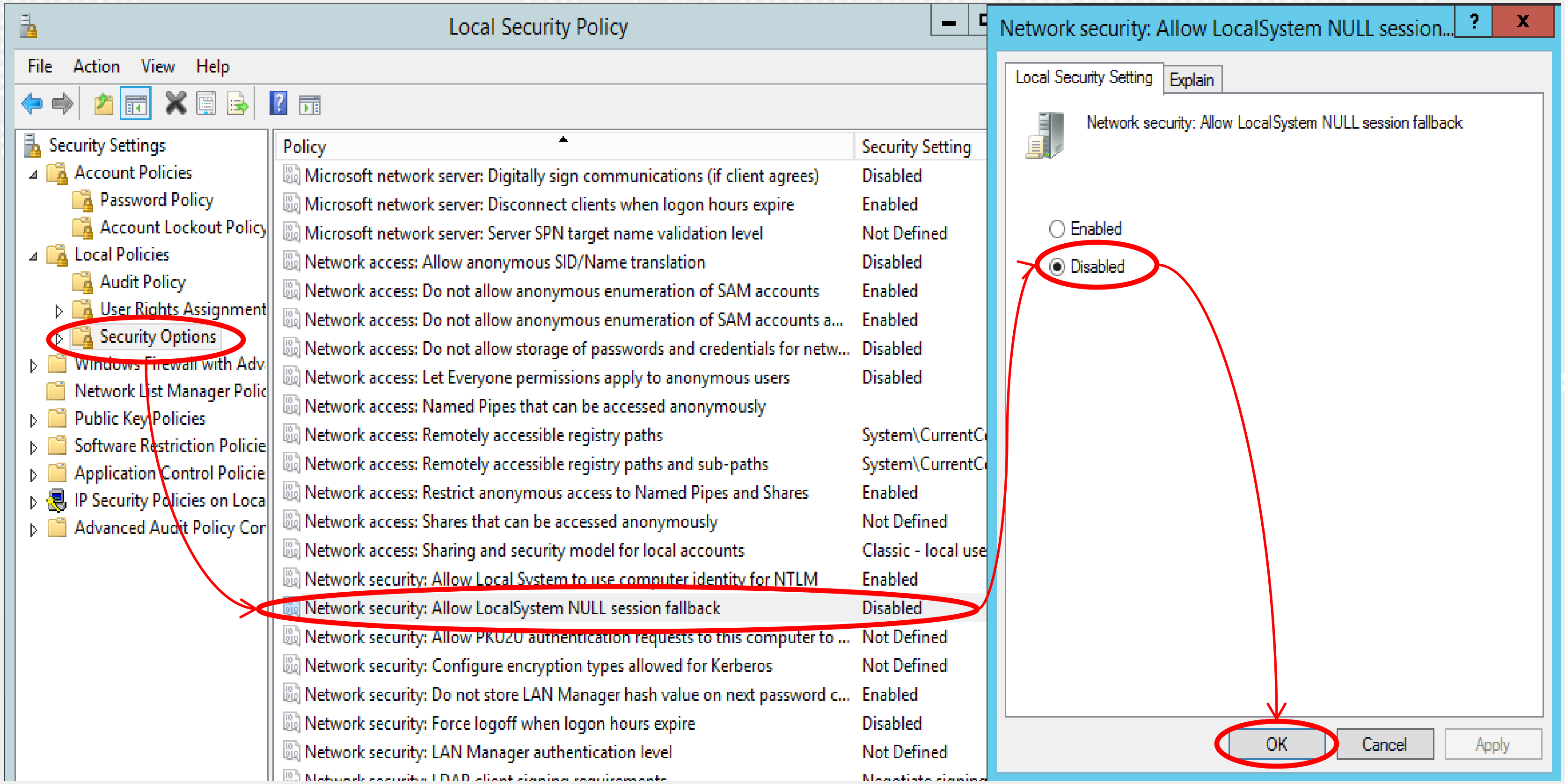
● Enabled

○ Disabled

MS Windows Server 2012

Security Options

Set 'Network security: Allow LocalSystem NULL session fallback' to 'Disabled'



Policy	Security Setting
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts a...	Enabled
Network access: Do not allow storage of passwords and credentials for netw...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
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
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing

Network security: Allow LocalSystem NULL session...

Network security: Allow LocalSystem NULL session fallback

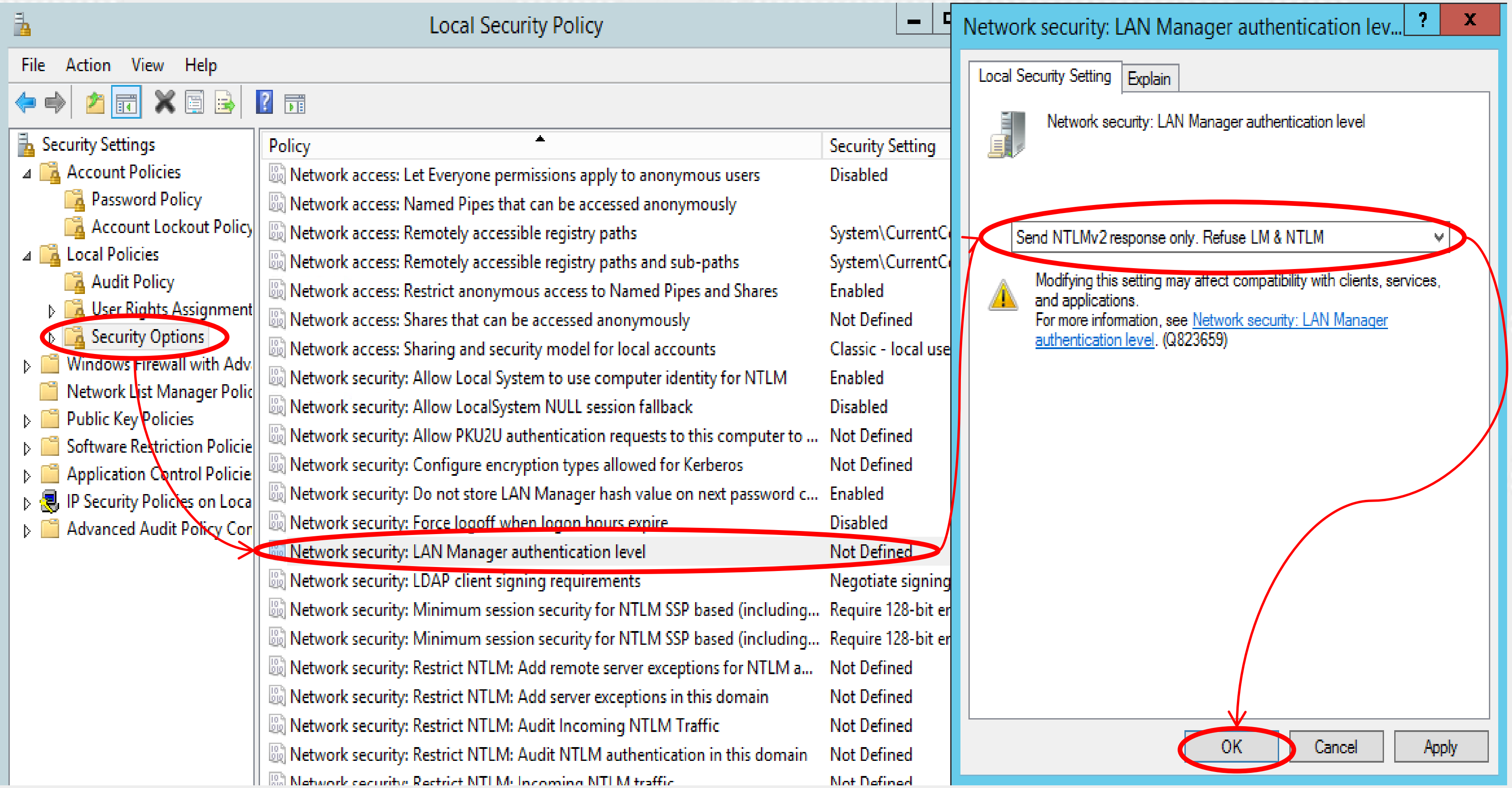
○ Enabled

● Disabled

MS Windows Server 2012

Security Options

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



Policy	Security Setting
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
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
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit er
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit er
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

Network security: LAN Manager authentication level

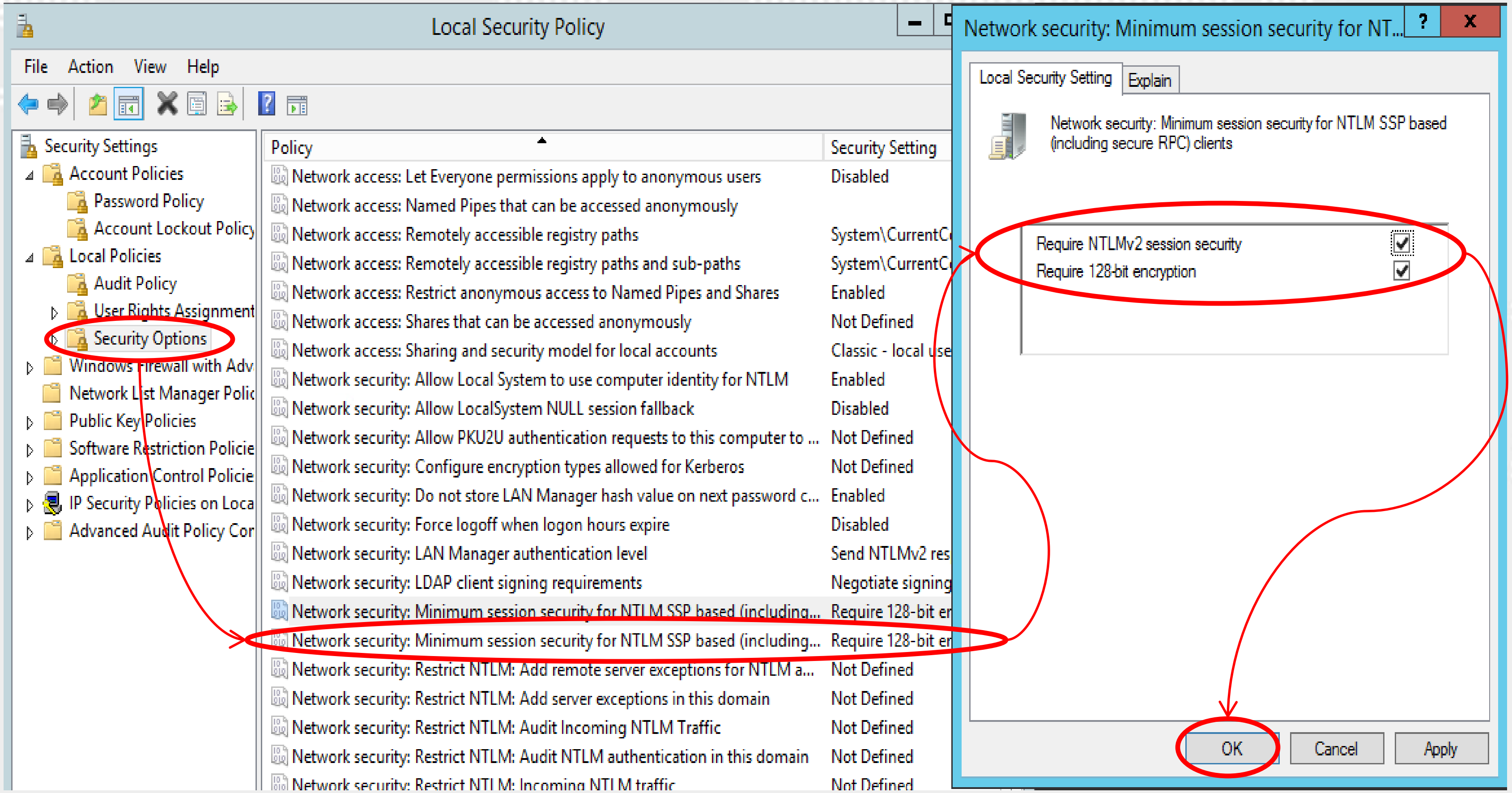
Send NTLMv2 response only. Refuse LM & NTLM

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)

MS Windows Server 2012

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



Local Security Policy

- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Adv
  - Network List Manager Polic
  - Public Key Policies
  - Software Restriction Policie
  - Application Control Policie
  - IP Security Policies on Loca
  - Advanced Audit Policy Cor

Policy	Security Setting
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
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
Network security: LAN Manager authentication level	Send NTLMv2 res
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

Network security: Minimum session security for NT...

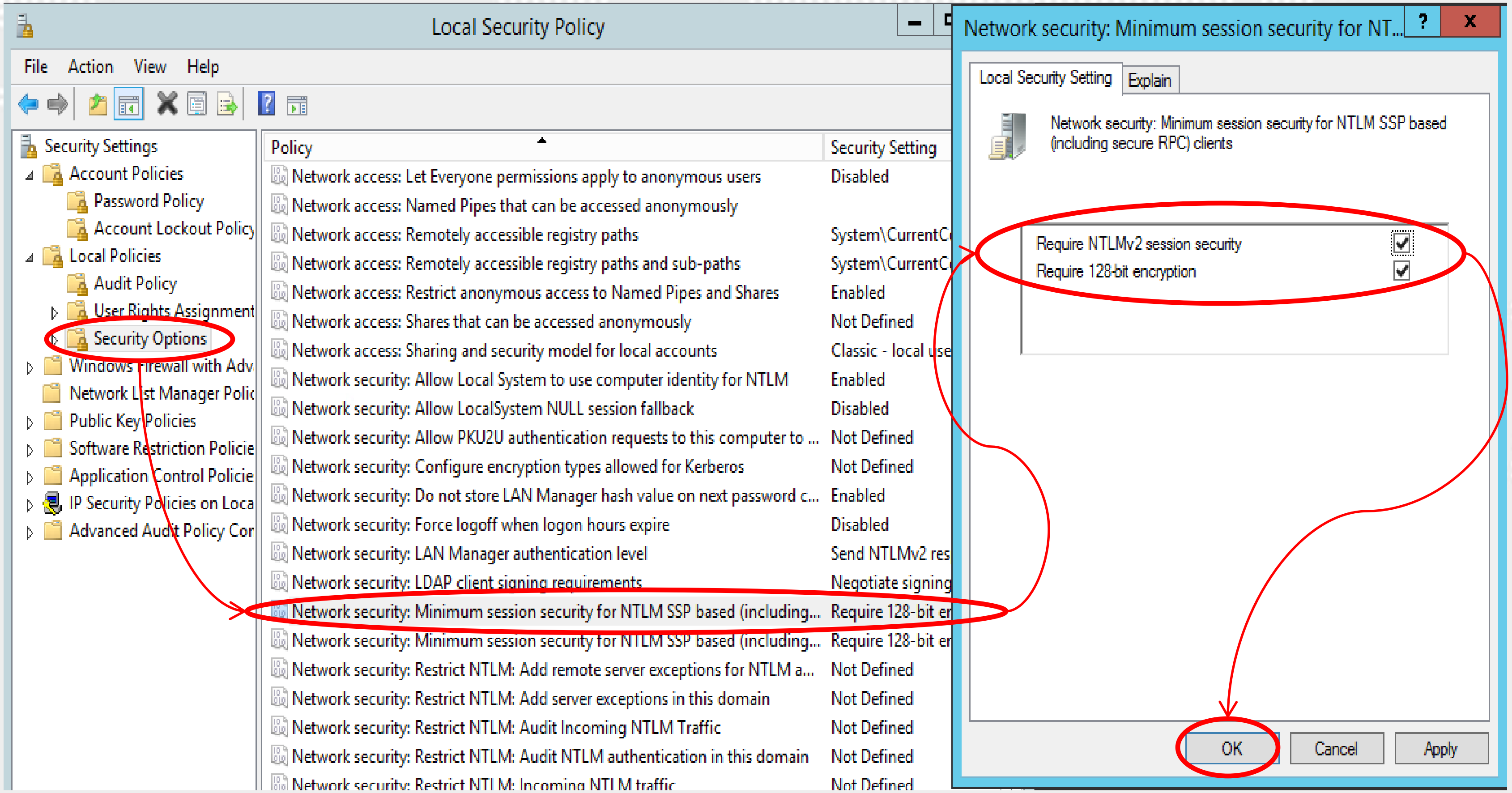
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

- ☑ Require NTLMv2 session security
- ☑ Require 128-bit encryption

MS Windows Server 2012

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'



Policy	Security Setting
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
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
Network security: LAN Manager authentication level	Send NTLMv2 res
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit er
Network security: Minimum session security for NTLM SSP based (including...	Require 128-bit er
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

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

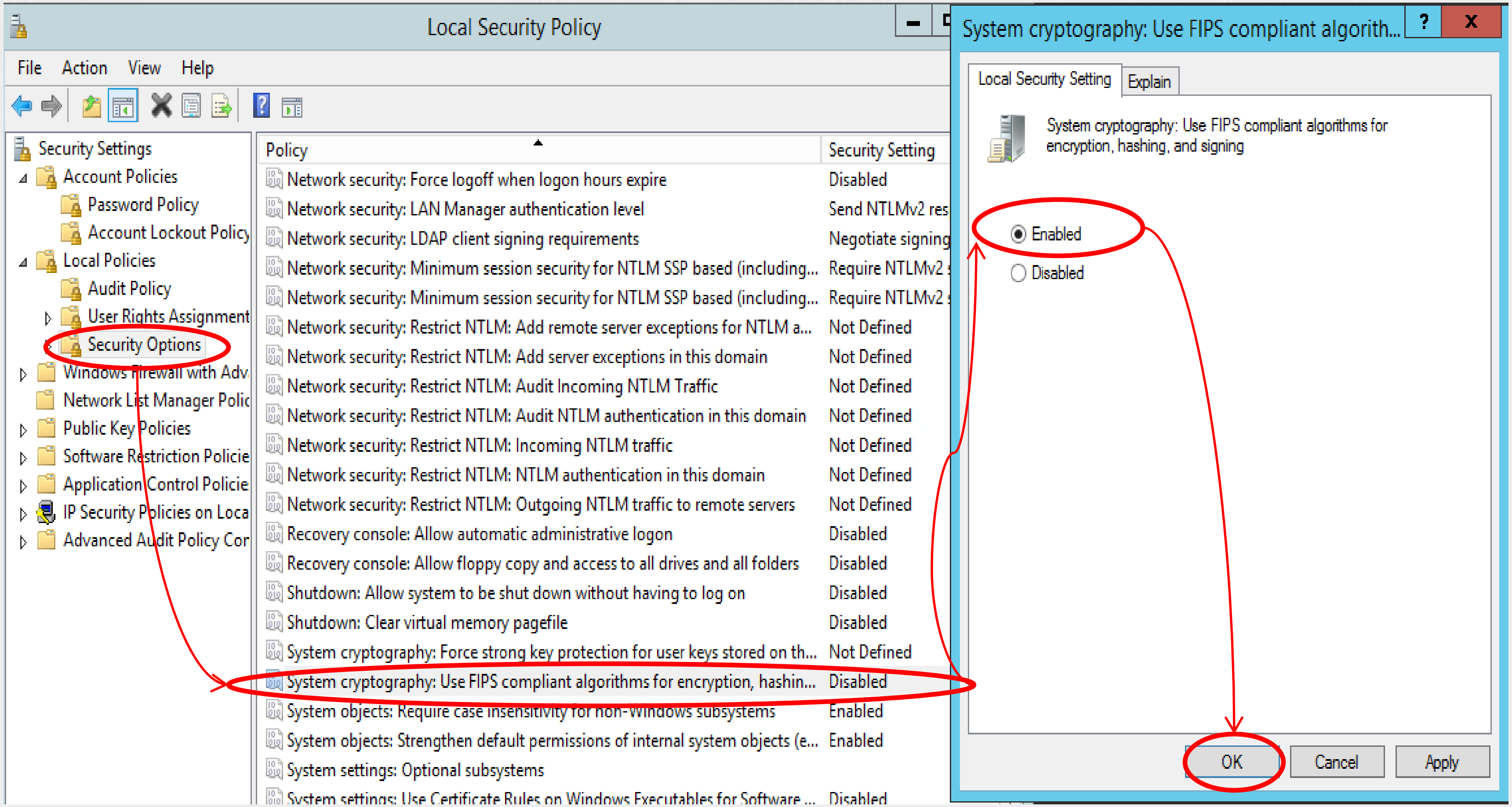
Require NTLMv2 session security ☑

Require 128-bit encryption ☑

MS Windows Server 2012

Security Options

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



Local Security Policy

- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Adv
  - Network List Manager Polic
  - Public Key Policies
  - Software Restriction Policie
  - Application Control Policie
  - IP Security Policies on Loca
  - Advanced Audit Policy Cor

Policy	Security Setting
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 res
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including...	Require NTLMv2 s
Network security: Minimum session security for NTLM SSP based (including...	Require NTLMv2 s
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
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on th...	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashin...	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executables for Software ...	Disabled

System cryptography: Use FIPS compliant algorith...

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

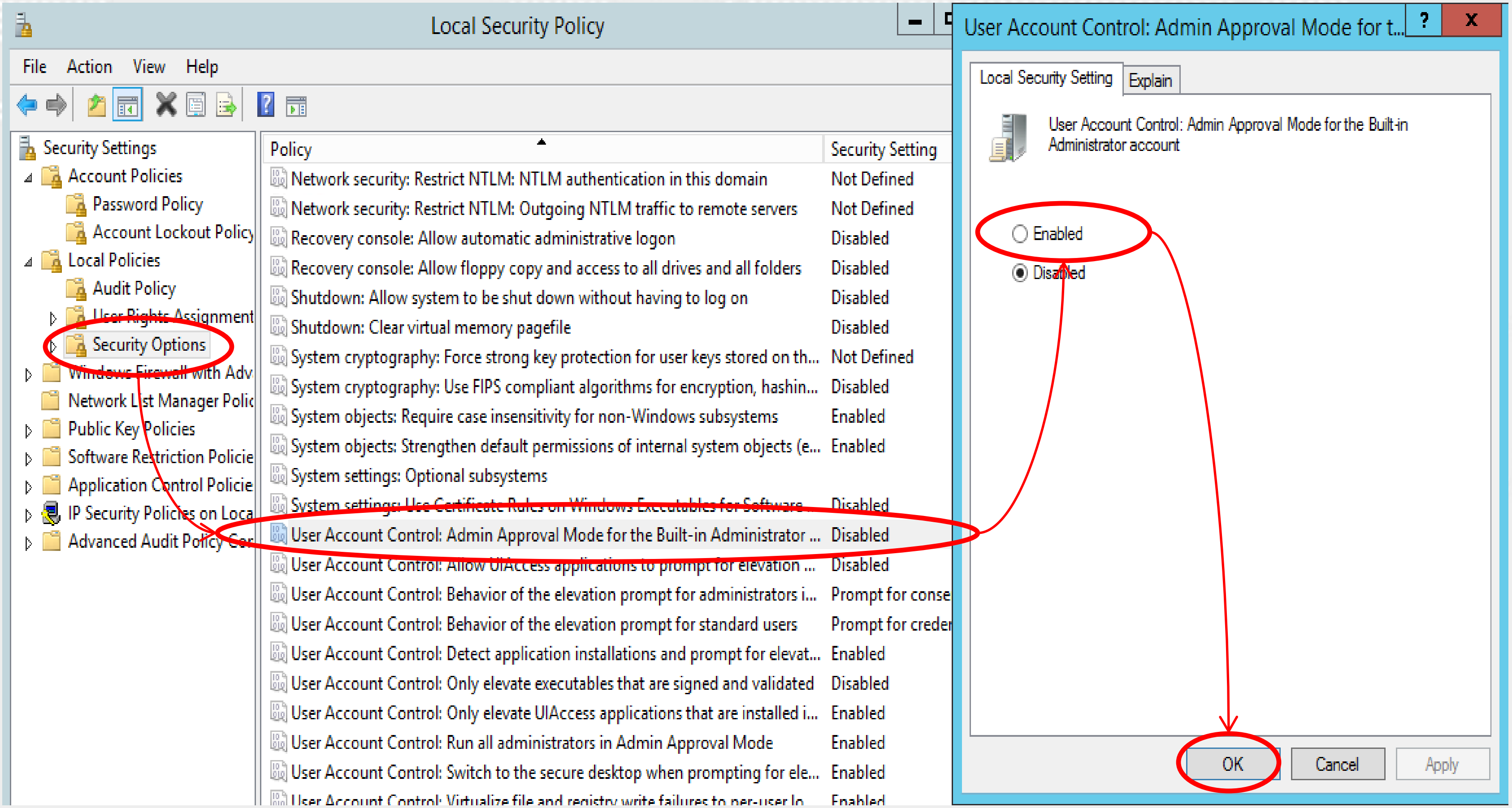
● Enabled

○ Disabled

MS Windows Server 2012

Security Options

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



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Adv
  - Network List Manager Polic
  - Public Key Policies
  - Software Restriction Policie
  - Application Control Policie
  - IP Security Policies on Loca
  - Advanced Audit Policy Cor

Policy	Security Setting
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on th...	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashin...	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executables for Software ...	Disabled
User Account Control: Admin Approval Mode for the Built-in Administrator ...	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation ...	Disabled
User Account Control: Behavior of the elevation prompt for administrators i...	Prompt for conse
User Account Control: Behavior of the elevation prompt for standard users	Prompt for creder
User Account Control: Detect application installations and prompt for elevat...	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed i...	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for ele...	Enabled
User Account Control: Virtualize file and registry write failures to per-user lo...	Enabled

User Account Control: Admin Approval Mode for t...

User Account Control: Admin Approval Mode for the Built-in Administrator account

○ Enabled

● Disabled

MS Windows Server 2012

Windows Components

AutoPlay Policies

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

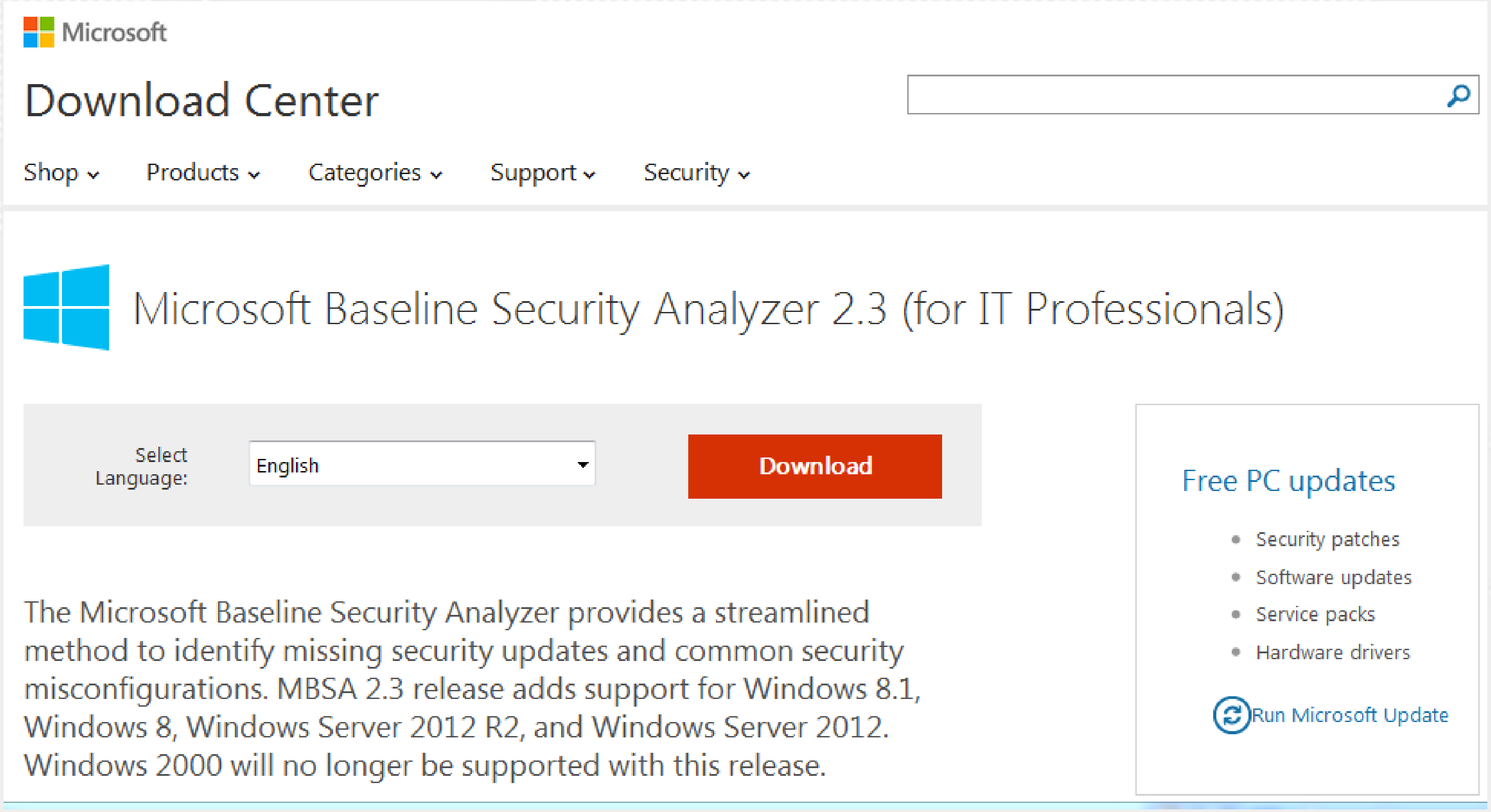
MS Windows Server 2012

Microsoft Baseline Security Analyzer

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

MS Windows Server 2012

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)

Select Language: English

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.

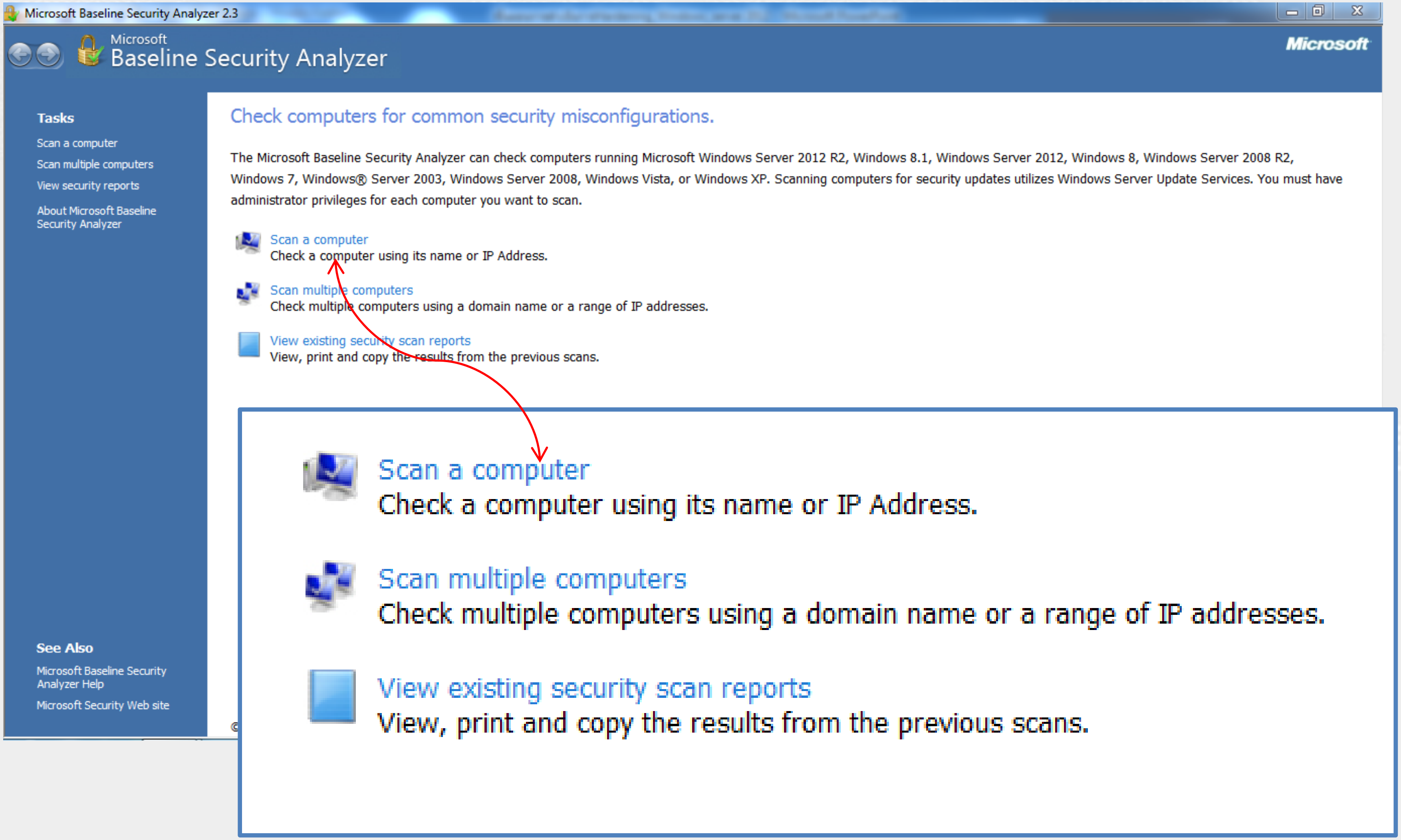
Free PC updates

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

Run Microsoft Update

MS Windows Server 2012

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Tasks

Scan a computer

Scan multiple computers

View security reports

About Microsoft Baseline Security Analyzer

See Also

Microsoft Baseline Security Analyzer Help

Microsoft Security Web site

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.

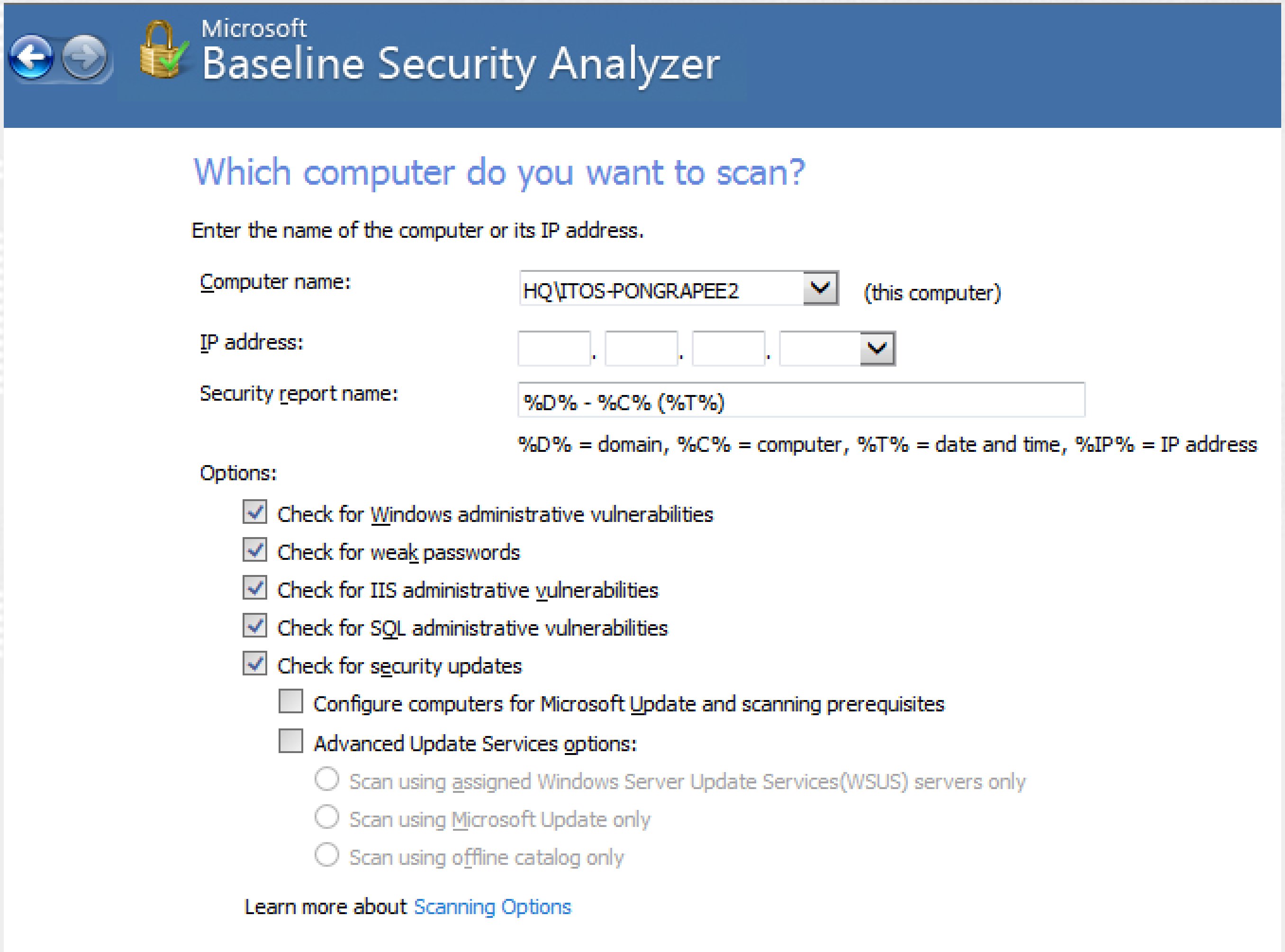
Scan a computer
Check a computer using its name or IP Address.

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.

MS Windows Server 2012

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: HQ\ITOS-PONGRAPEE2 (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

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

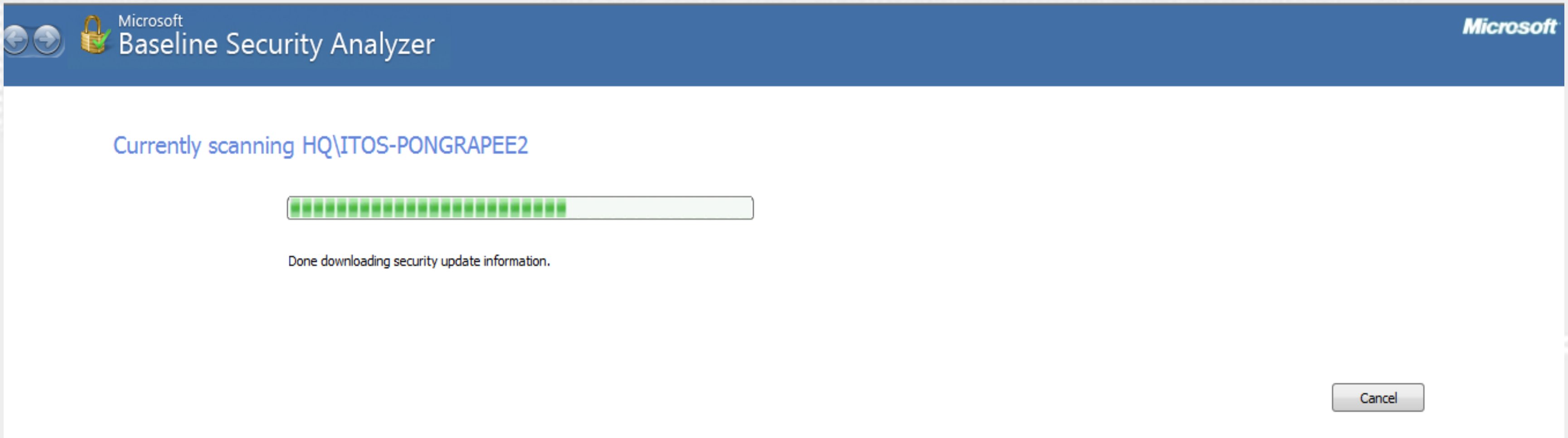
Options:

- ☑ 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

MS Windows Server 2012

Microsoft Baseline Security Analyzer

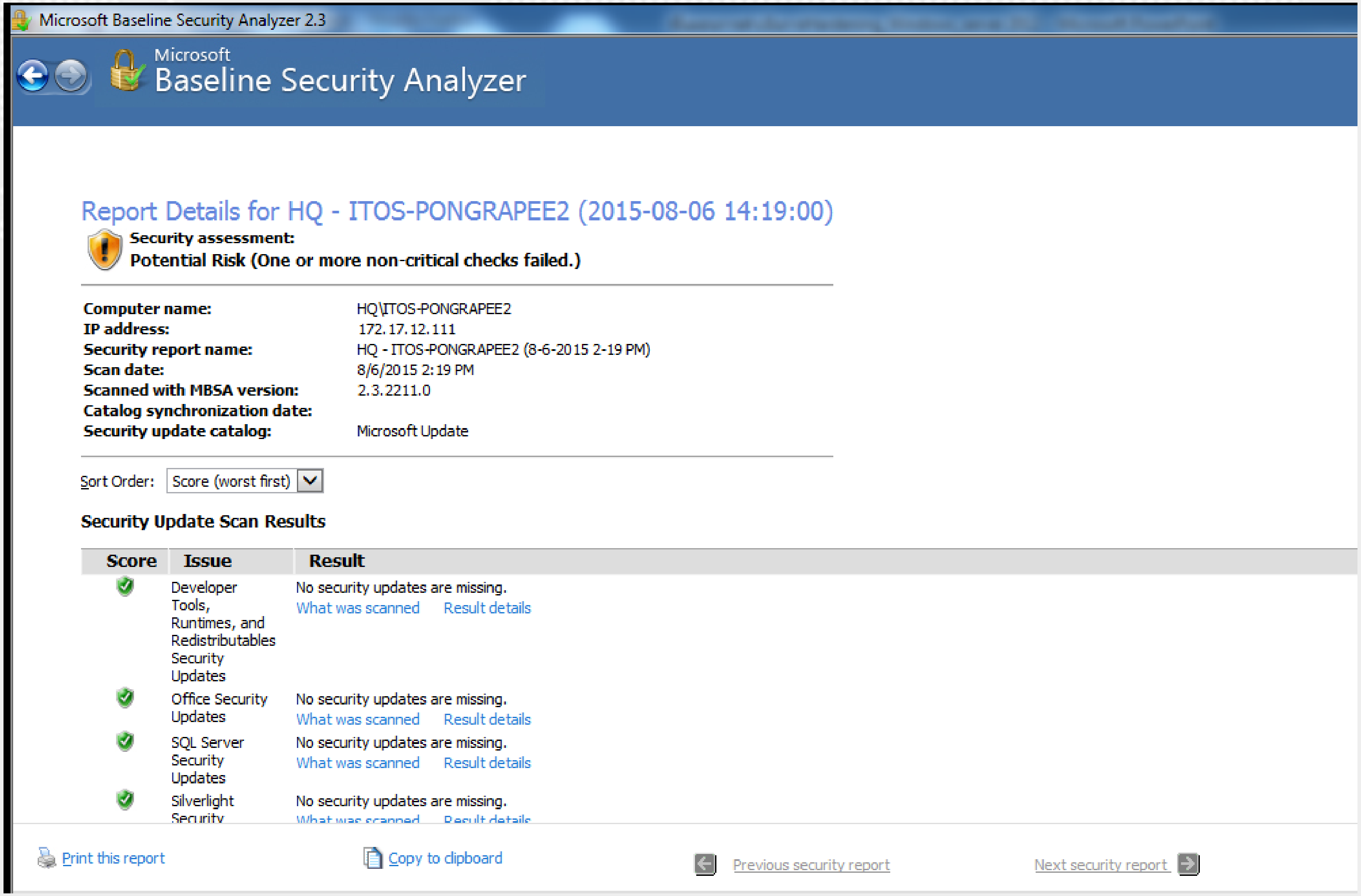


Currently scanning HQ\ITOS-PONGRAPEE2

Done downloading security update information.

MS Windows Server 2012

Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer 2.3

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: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✓	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
✓	Office Security Updates	No security updates are missing. What was scanned Result details
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details
✓	Silverlight Security	No security updates are missing. What was scanned Result details

MS Windows Server 2012

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'

MS Windows Server 2012

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'

MS Windows Server 2012

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)

MS Windows Server 2012

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

MS Windows Server 2012

Summery

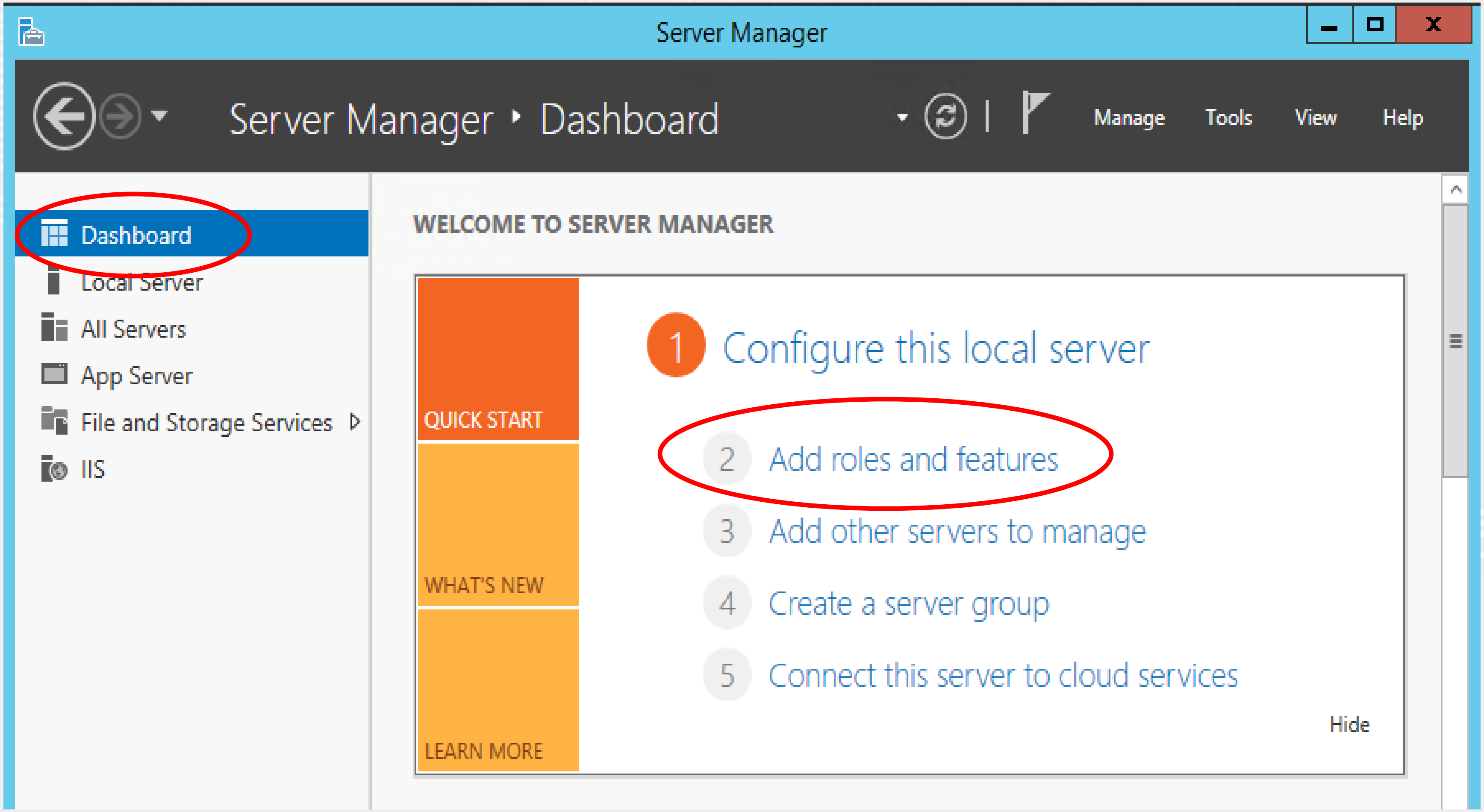
- Set 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' to 'Require NTLMv2 session security,Require 128-bit encryption'
- Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'
- Set 'User Account Control: 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)

Secure FTP Server on Windows Using IIS

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

IIS Server



Server Manager

Server Manager ‣ Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

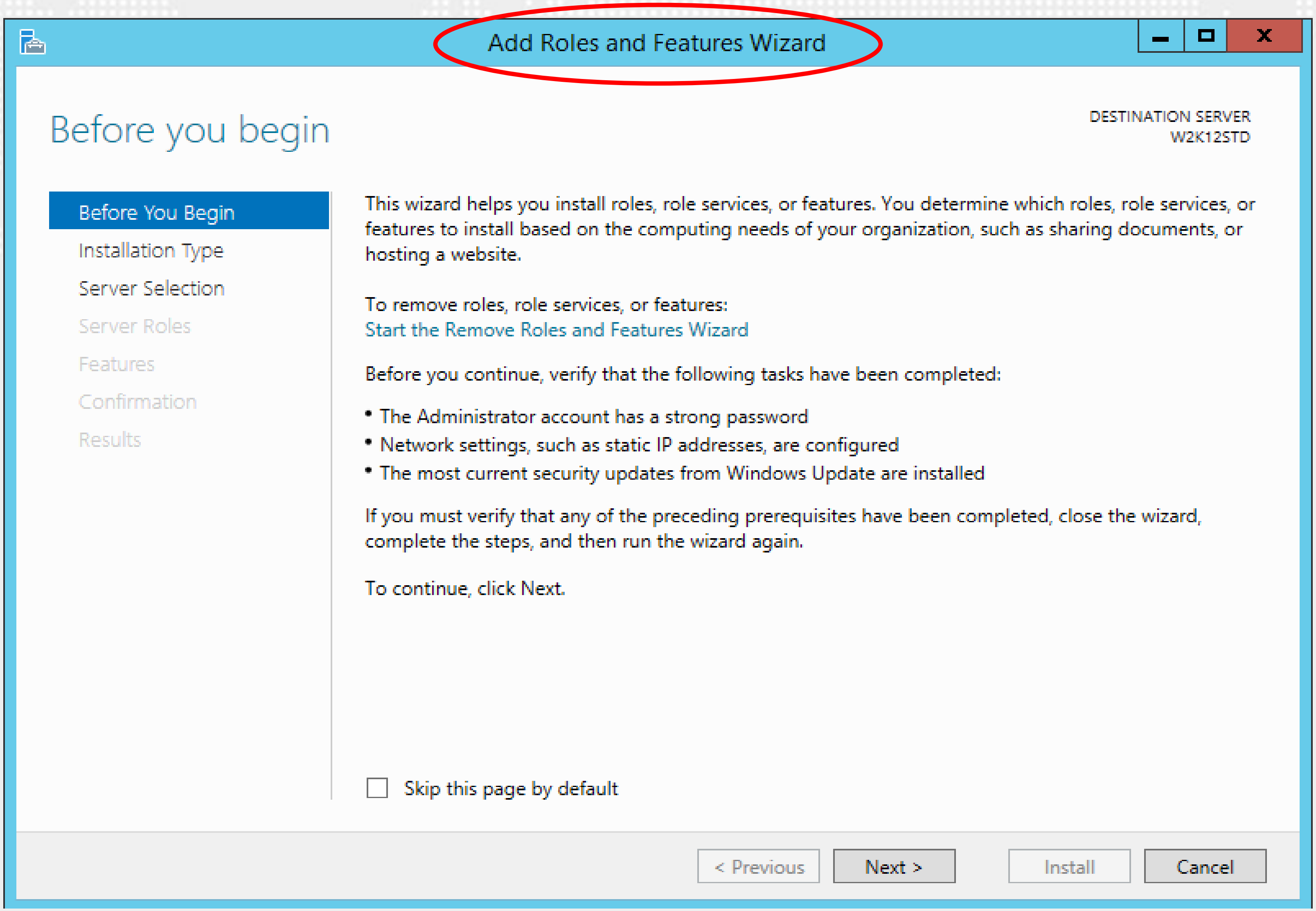
4 Create a server group

5 Connect this server to cloud services

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Add Roles and Features



Before you begin

DESTINATION SERVER
W2K12STD

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

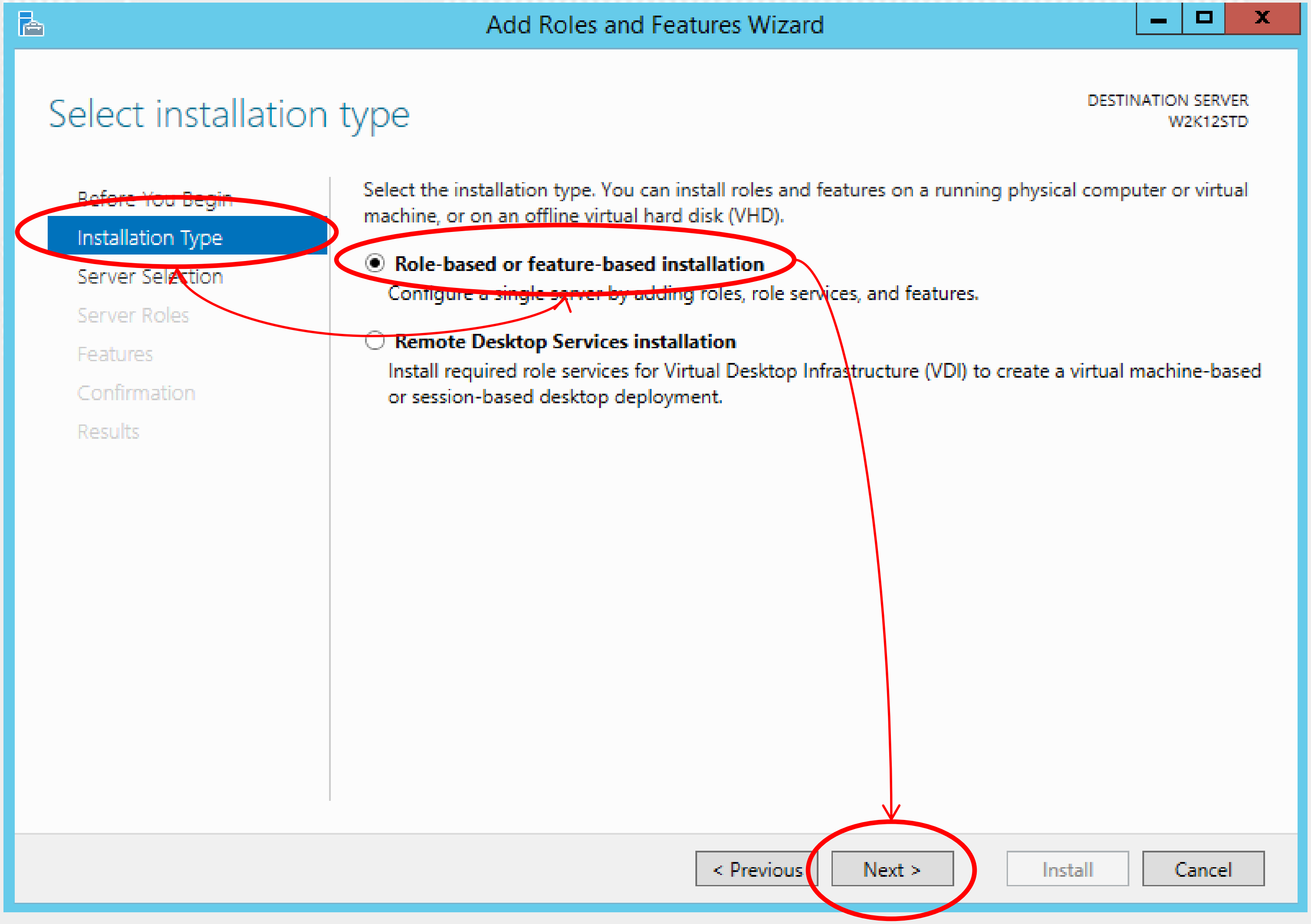
To continue, click Next.

□ Skip this page by default

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Installation Type



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
W2K12STD

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

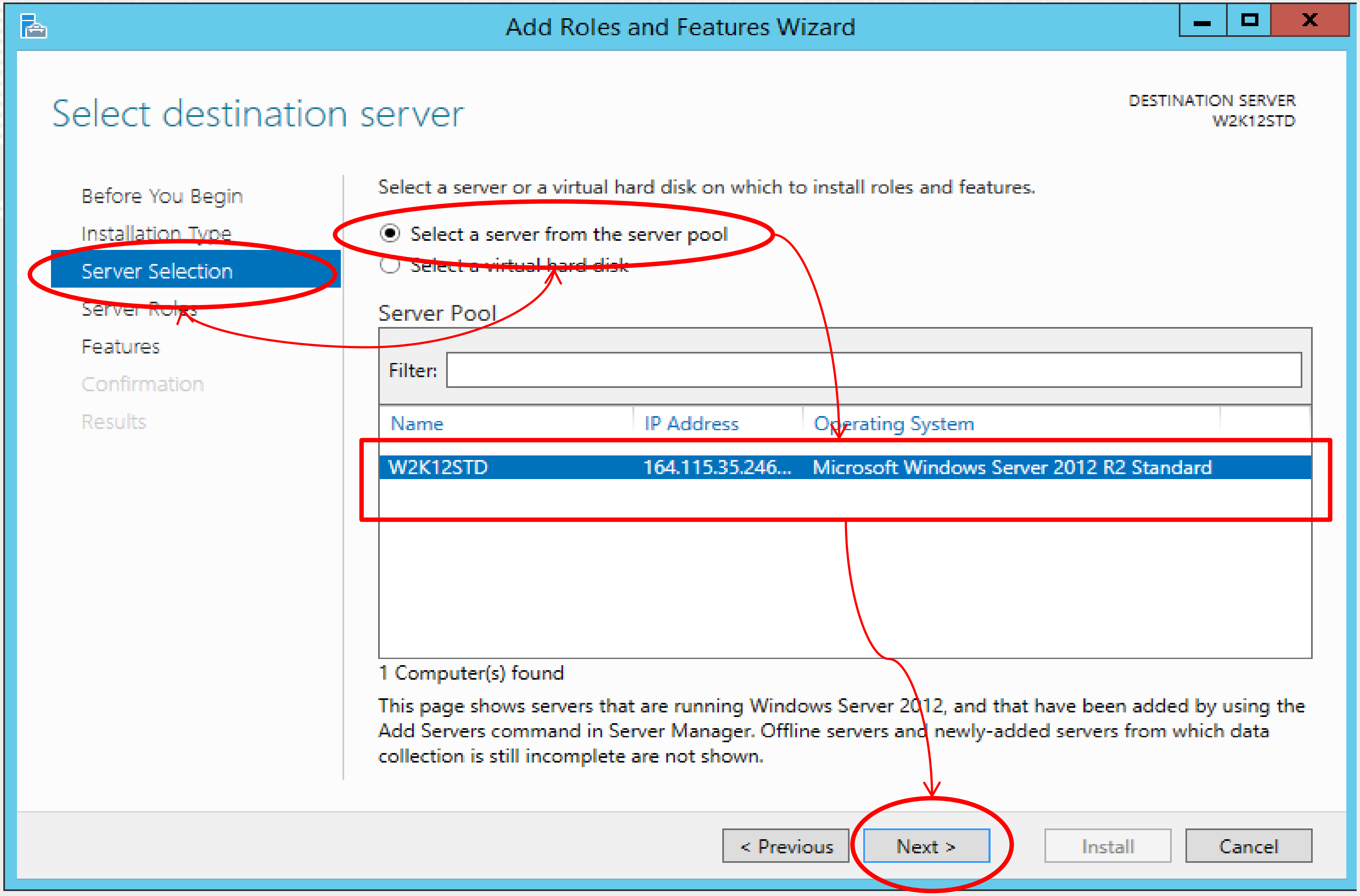
● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Installation Type



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
W2K12STD

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool

○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
W2K12STD	164.115.35.246...	Microsoft Windows Server 2012 R2 Standard

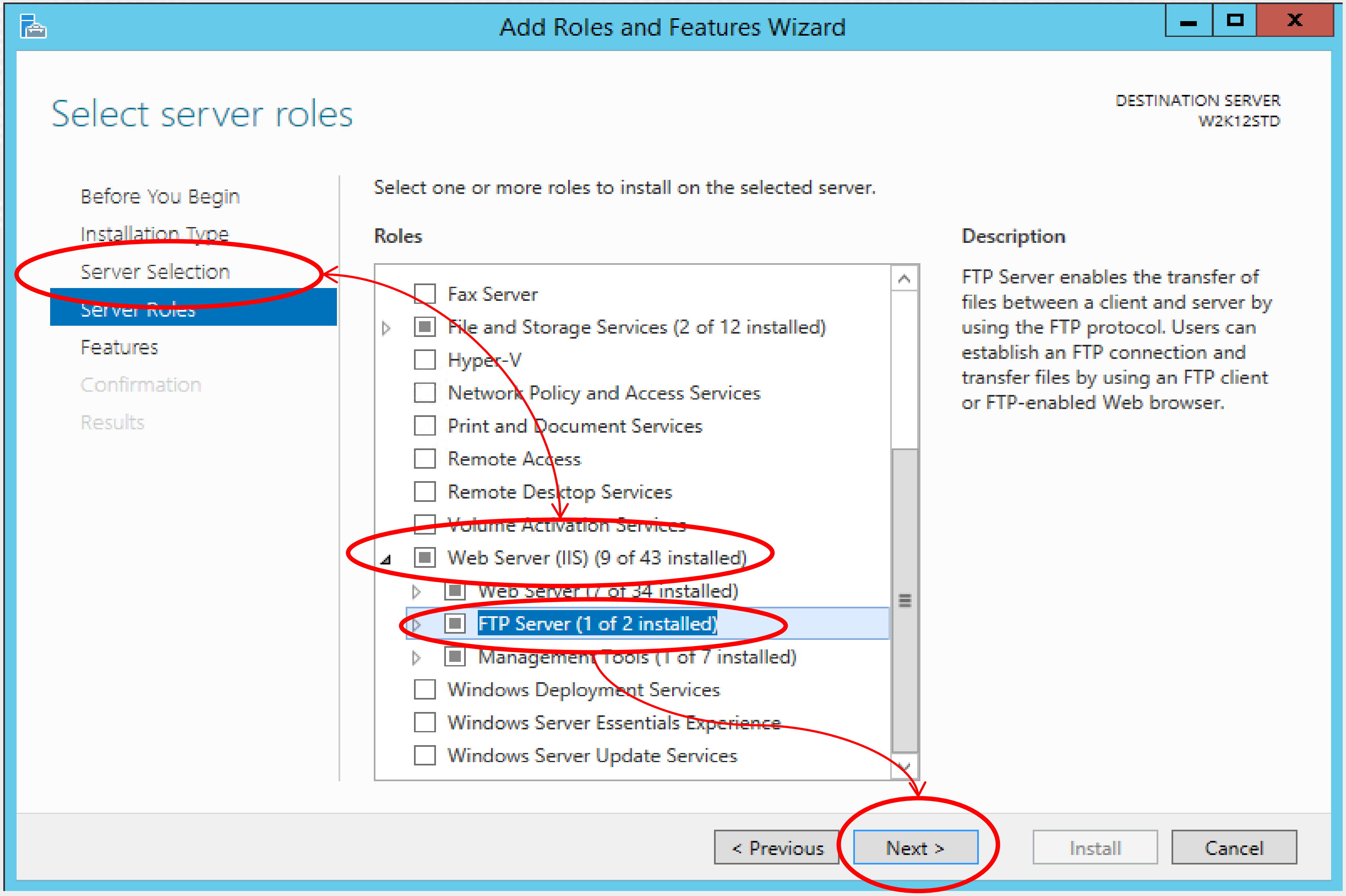
1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Installation Type



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
W2K12STD

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

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

Roles

- □ Fax Server
- ▨ File and Storage Services (2 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ▨ Web Server (IIS) (9 of 43 installed)
  - ▨ Web Server (7 of 34 installed)
  - ▨ FTP Server (1 of 2 installed)
  - ▨ Management Tools (1 of 7 installed)
- □ Windows Deployment Services
- □ Windows Server Essentials Experience
- □ Windows Server Update Services

Description

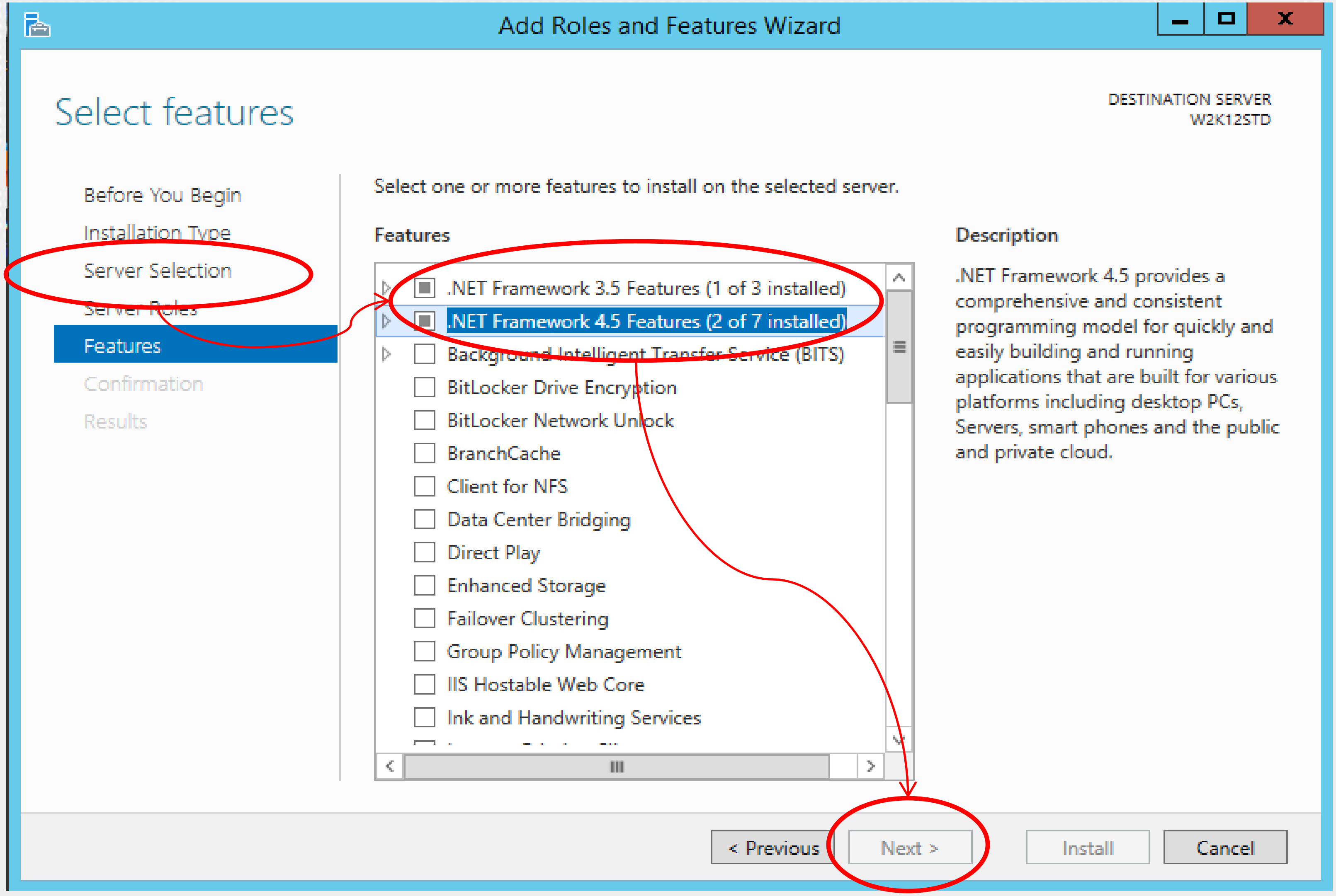
FTP Server enables the transfer of files between a client and server by using the FTP protocol. Users can establish an FTP connection and transfer files by using an FTP client or FTP-enabled Web browser.

< Previous | Next > | Install | Cancel

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Installation Type



Add Roles and Features Wizard

Select features

DESTINATION SERVER
W2K12STD

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

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

Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- □ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

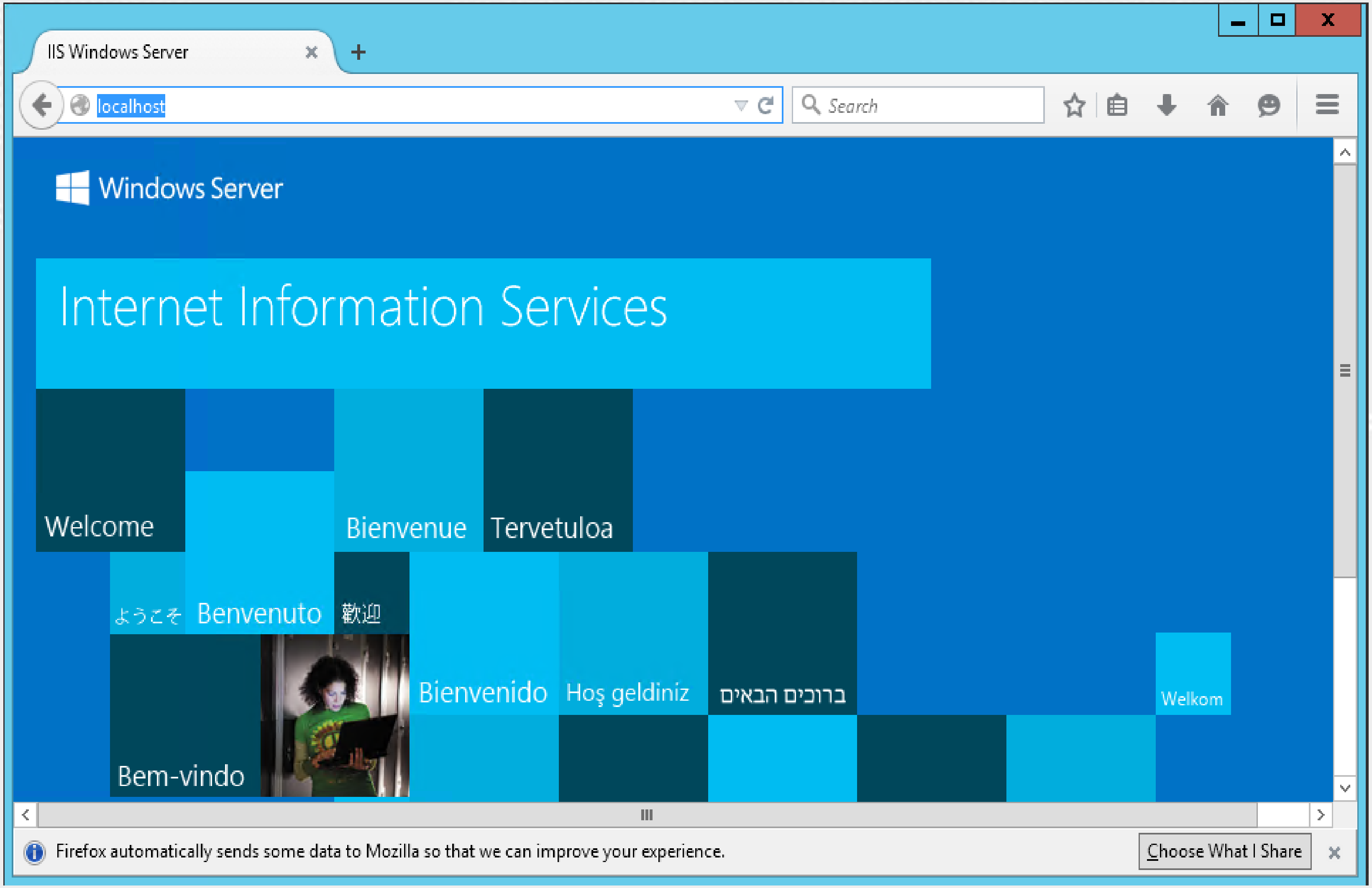
Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

IIS Start Services

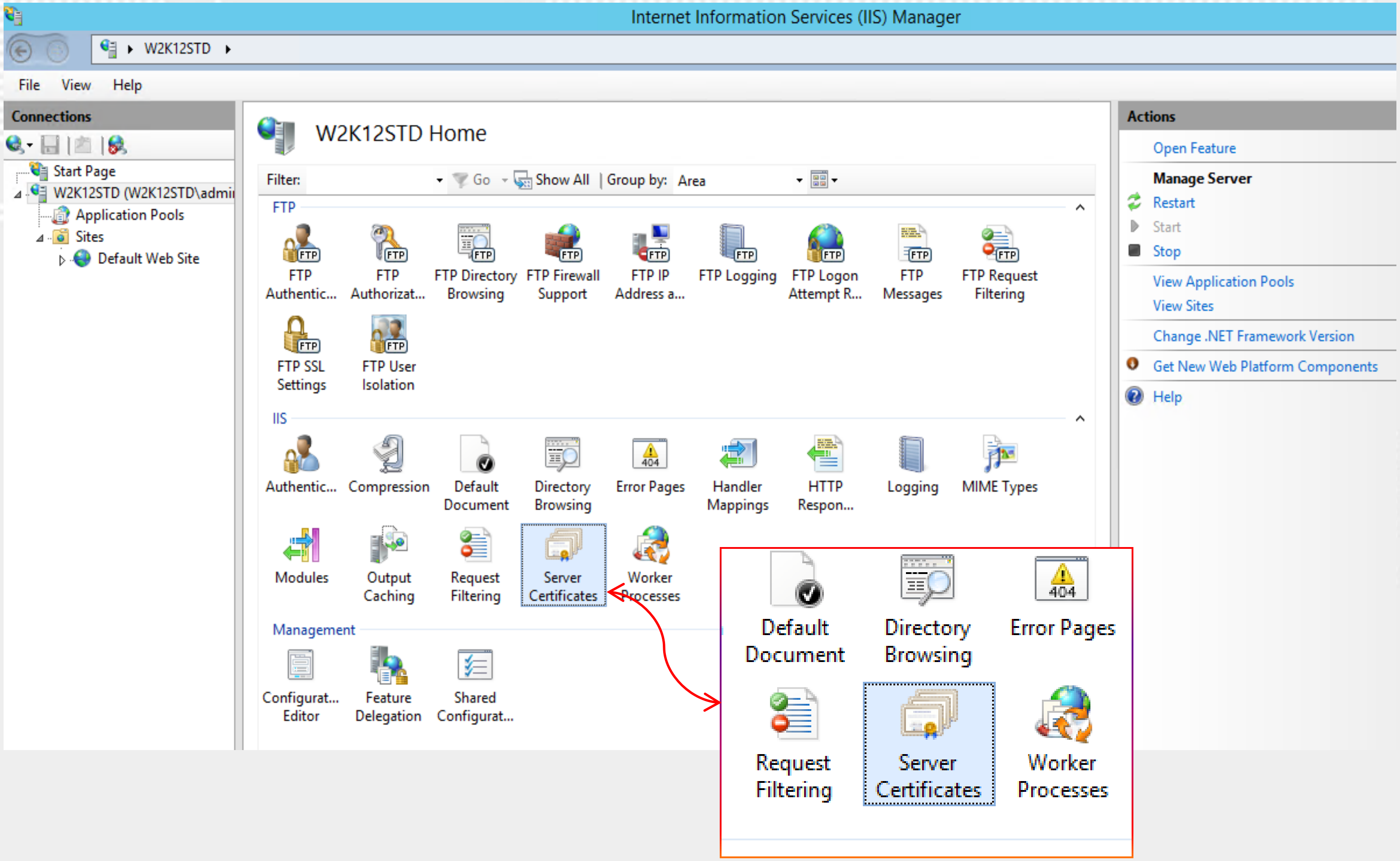


Firefox automatically sends some data to Mozilla so that we can improve your experience.

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

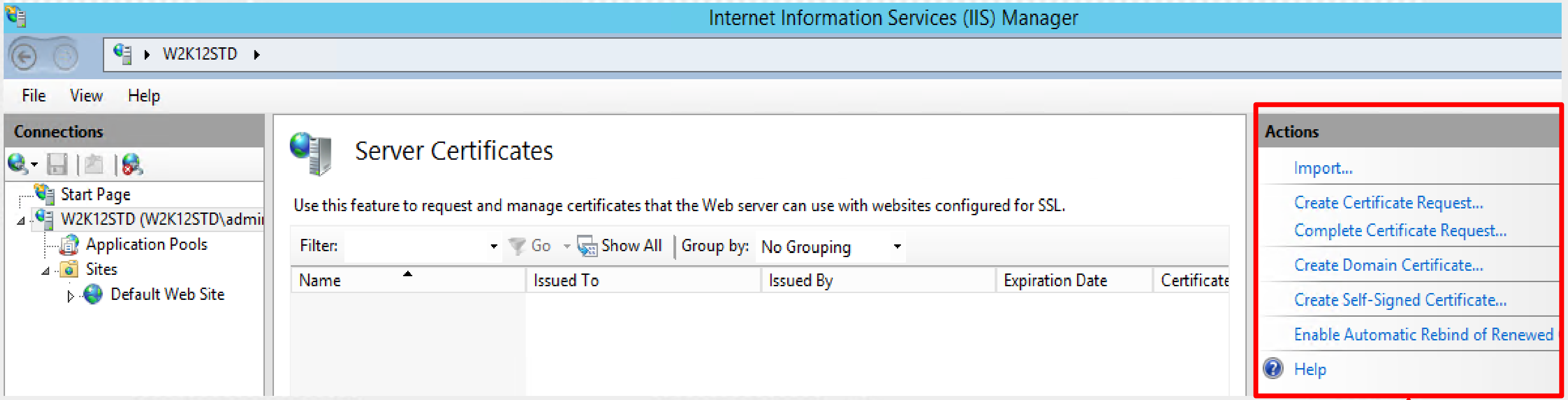
Server Certificates



MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create Certificates



Server Certificates

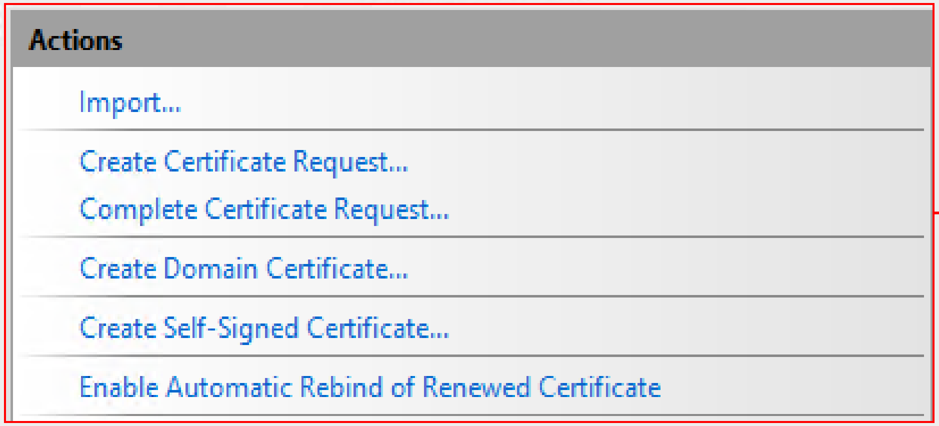
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate

Actions

- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- Enable Automatic Rebind of Renewed
- Help



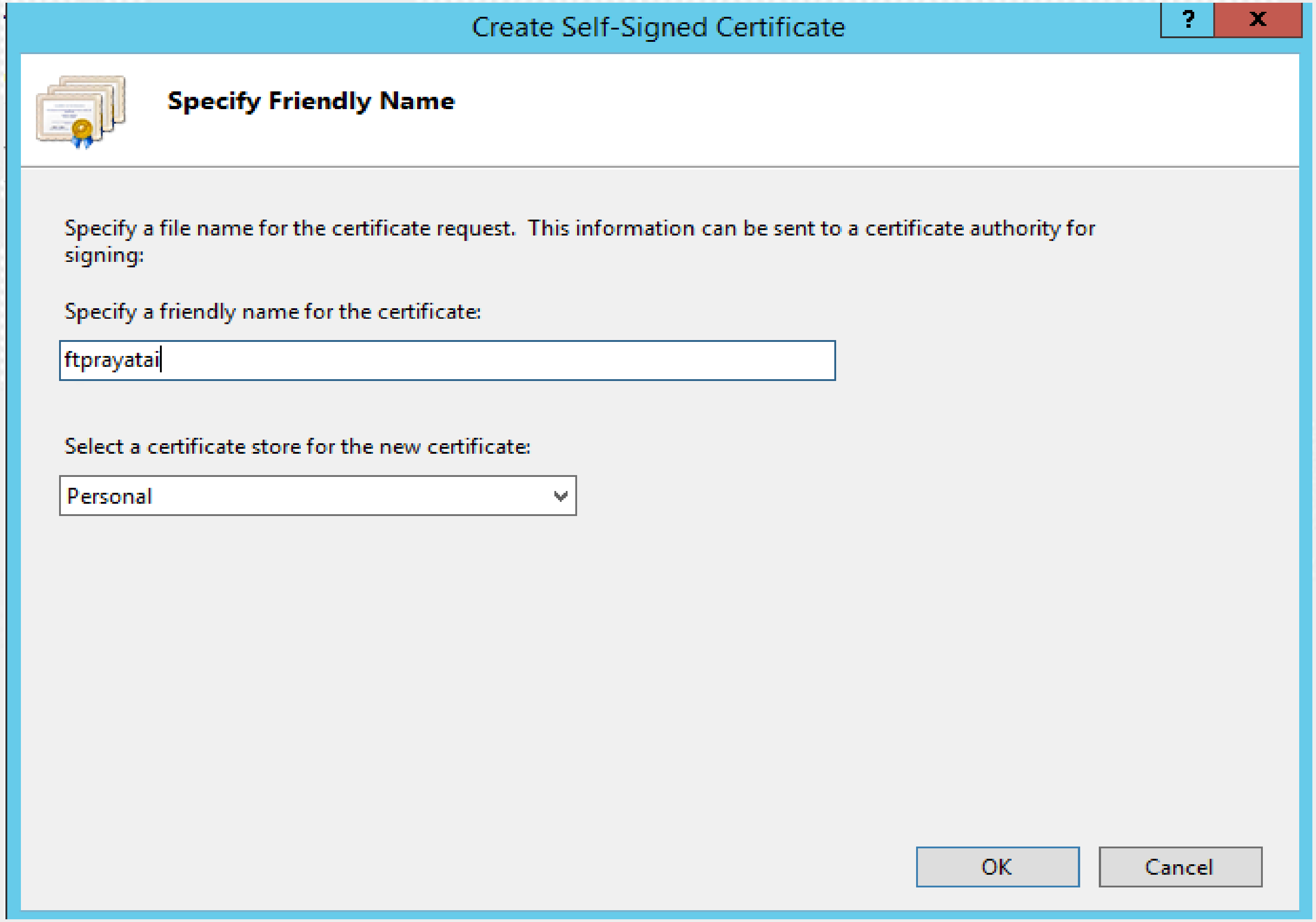
Actions

- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- Enable Automatic Rebind of Renewed Certificate

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create Self-signed Certificate



Create Self-Signed Certificate

Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

ftprayatai

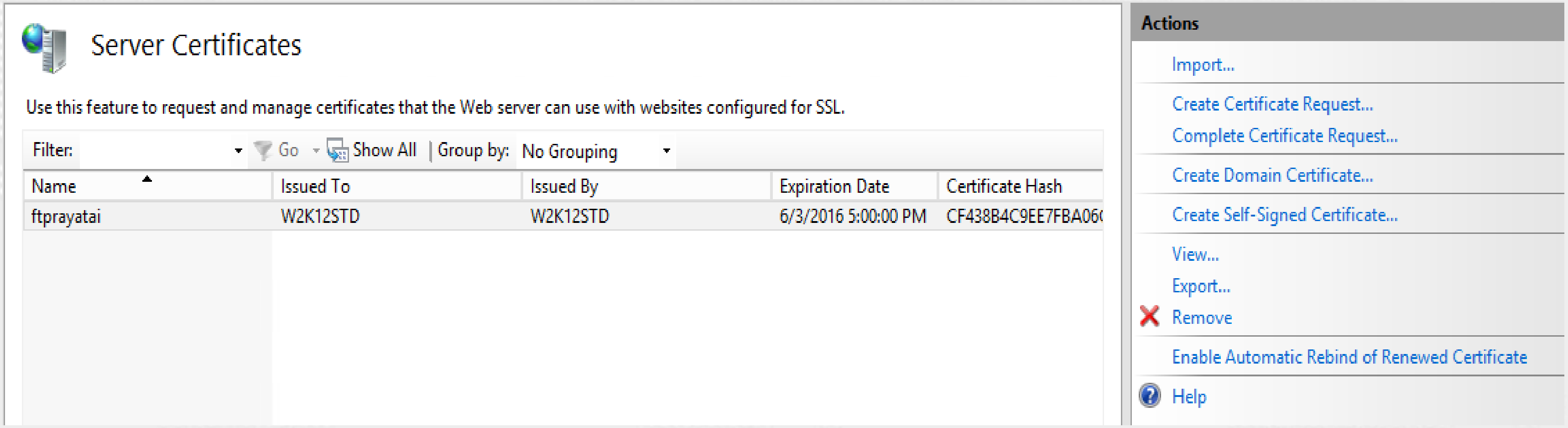
Select a certificate store for the new certificate:

Personal

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create Self-signed Certificate


Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

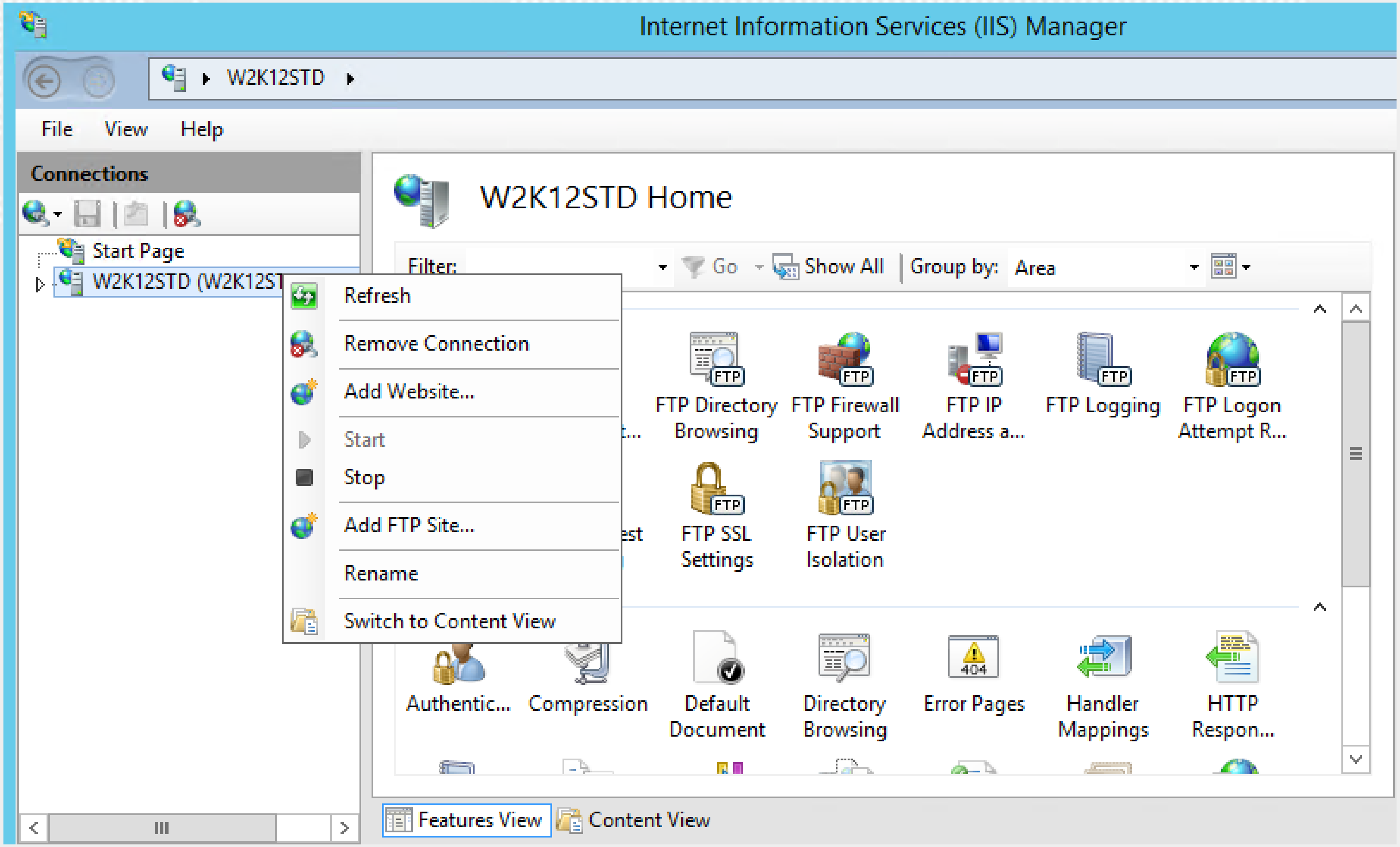
Filter:
Go
Show All
Group by: No Grouping
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help

Name	Issued To	Issued By	Expiration Date	Certificate Hash
ftprayatai	W2K12STD	W2K12STD	6/3/2016 5:00:00 PM	CF438B4C9EE7FBA06

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

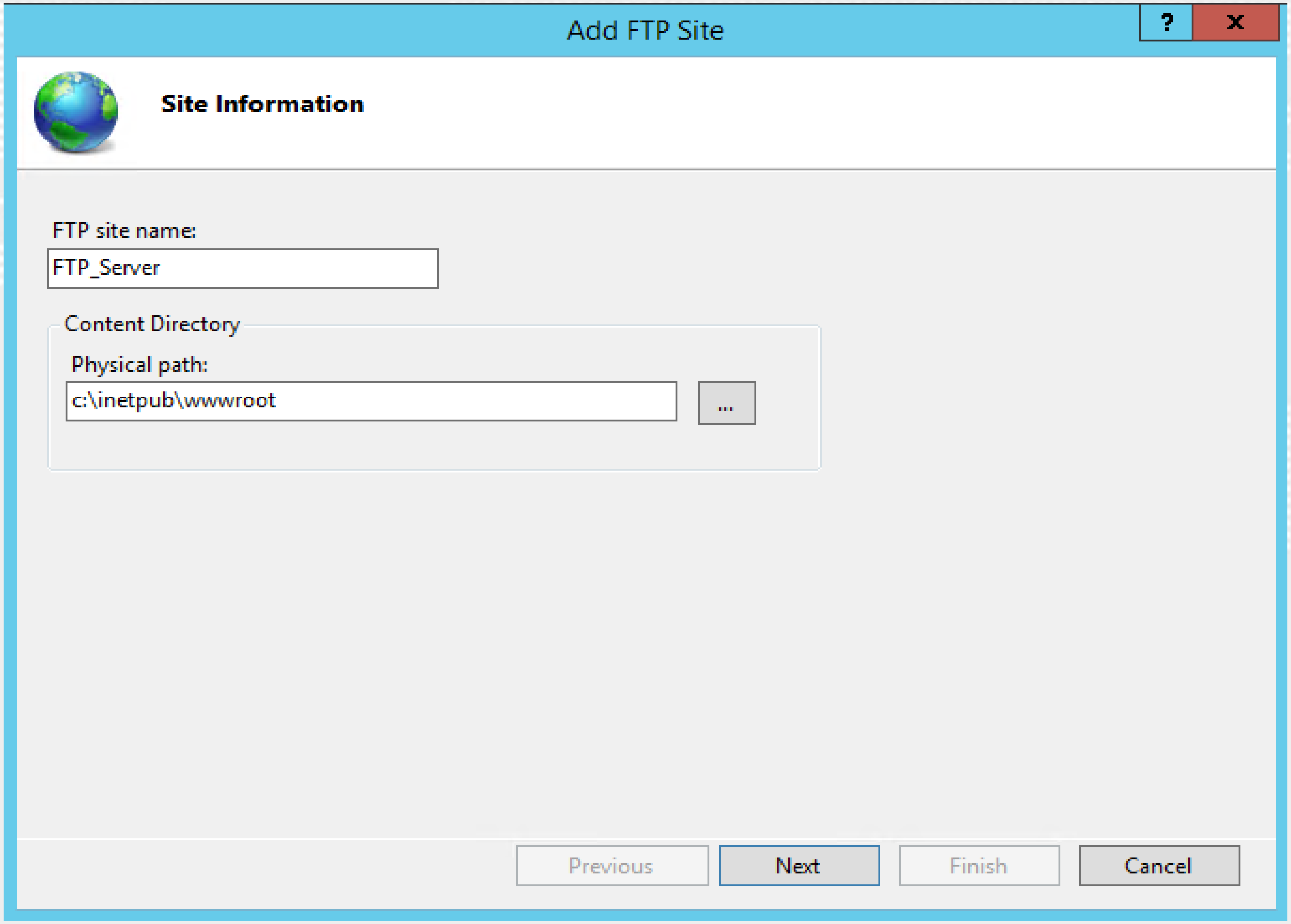
Create FTP site



MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create FTP site



Add FTP Site

Site Information

FTP site name: FTP_Server

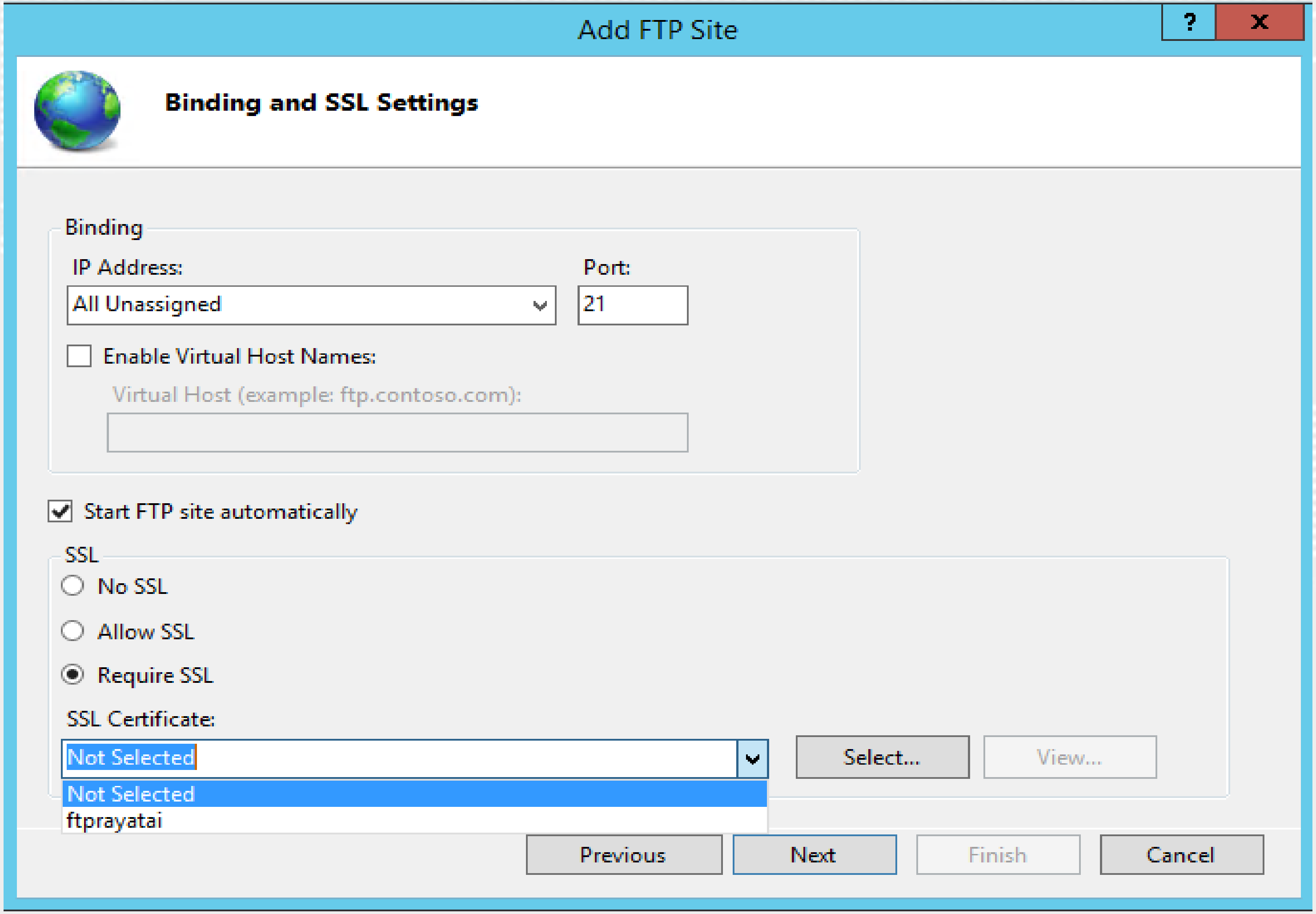
Content Directory

Physical path: c:\inetpub\wwwroot

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create FTP site



Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

○ No SSL

○ Allow SSL

● Require SSL

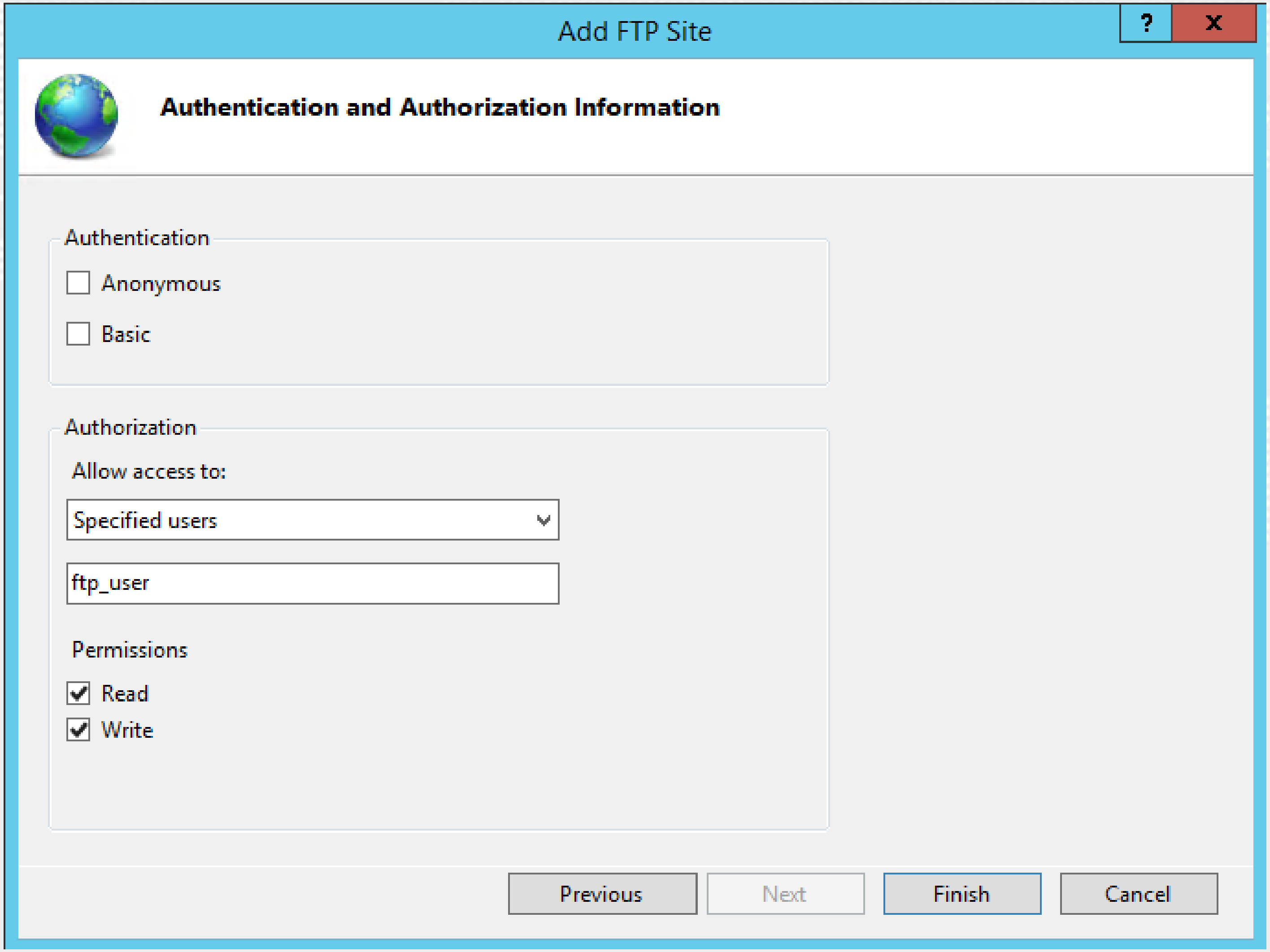
SSL Certificate: Not Selected

- Not Selected
- ftprayatai

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Create FTP site



Add FTP Site

Authentication and Authorization Information

Authentication

□ Anonymous

□ Basic

Authorization

Allow access to:

Specified users

ftp_user

Permissions

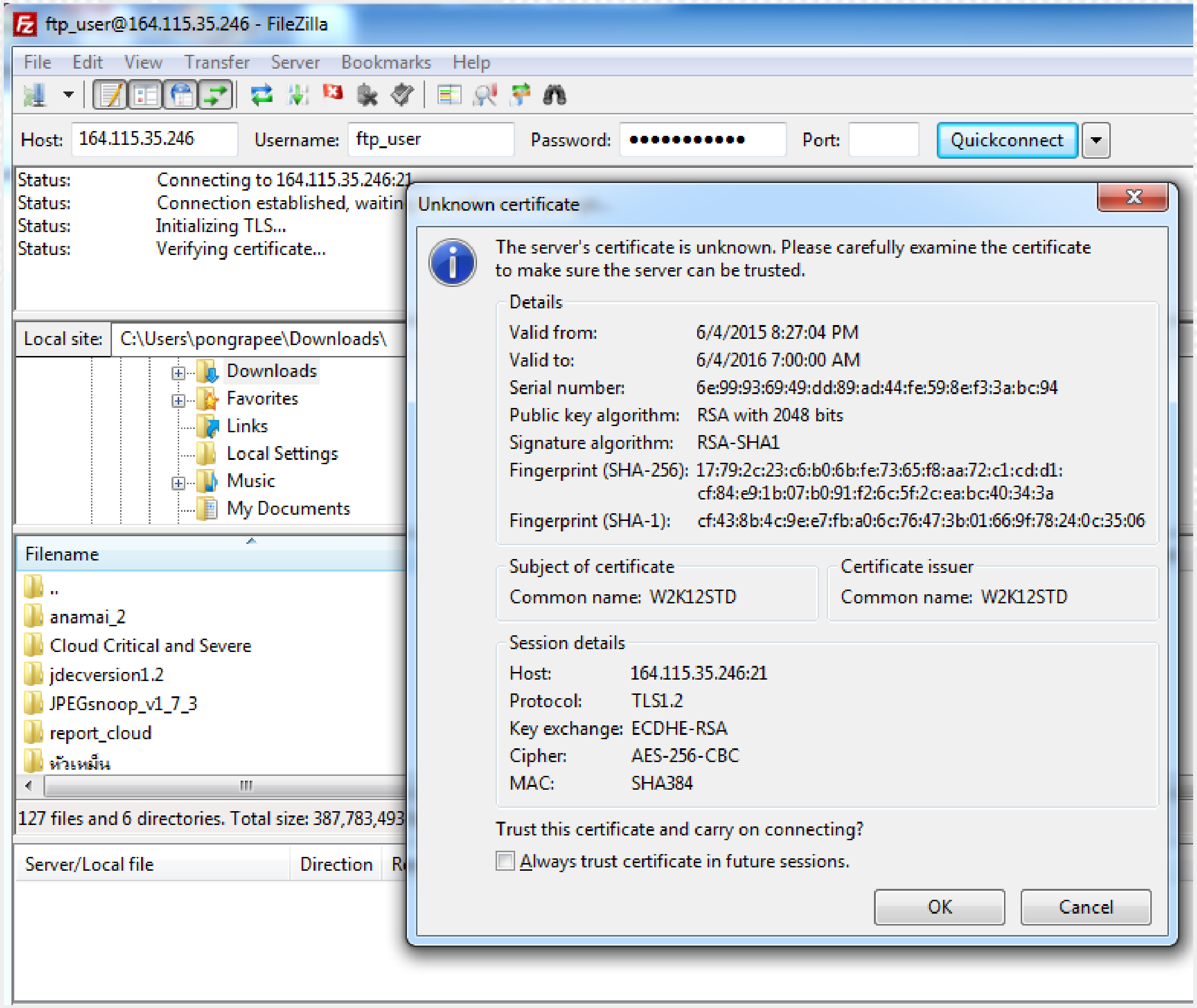
☑ Read

☑ Write

MS Windows Server 2012

Installing Secure FTP Server on Windows Using IIS

Login FTP site



Host: 164.115.35.246 Username: ftp_user Password: ●●●●●●●●●●●● Port:

```
Status:     Connecting to 164.115.35.246:21
Status:     Connection established, waitin
Status:     Initializing TLS...
Status:     Verifying certificate...
```

Local site: C:\Users\pongrapee\Downloads\

- Downloads
- Favorites
- Links
- Local Settings
- Music
- My Documents

Filename

- ..
- anamai_2
- Cloud Critical and Severe
- jdecversion1.2
- JPEGsnoop_v1_7_3
- report_cloud
- หัวเหมีน

127 files and 6 directories. Total size: 387,783,493

Unknown certificate

The server's certificate is unknown. Please carefully examine the certificate to make sure the server can be trusted.

Details

Valid from:	6/4/2015 8:27:04 PM
Valid to:	6/4/2016 7:00:00 AM
Serial number:	6e:99:93:69:49:dd:89:ad:44:fe:59:8e:f3:3a:bc:94
Public key algorithm:	RSA with 2048 bits
Signature algorithm:	RSA-SHA1
Fingerprint (SHA-256):	17:79:2c:23:c6:b0:6b:fe:73:65:f8:aa:72:c1:cd:d1: cf:84:e9:1b:07:b0:91:f2:6c:5f:2c:ea:bc:40:34:3a
Fingerprint (SHA-1):	cf:43:8b:4c:9e:e7:fb:a0:6c:76:47:3b:01:66:9f:78:24:0c:35:06

Subject of certificate

Common name: W2K12STD

Certificate issuer

Common name: W2K12STD

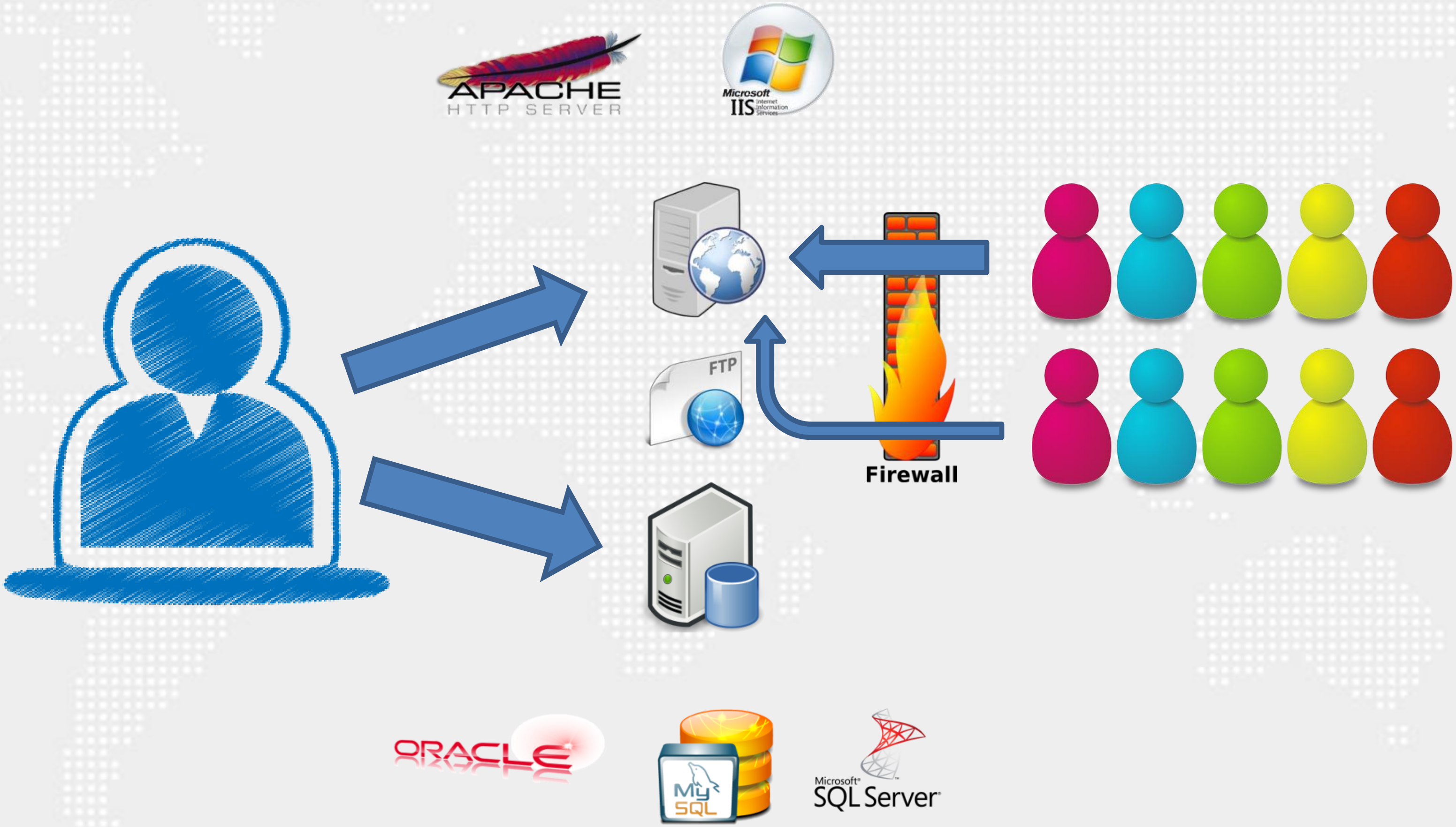
Session details

Host:	164.115.35.246:21
Protocol:	TLS1.2
Key exchange:	ECDHE-RSA
Cipher:	AES-256-CBC
MAC:	SHA384

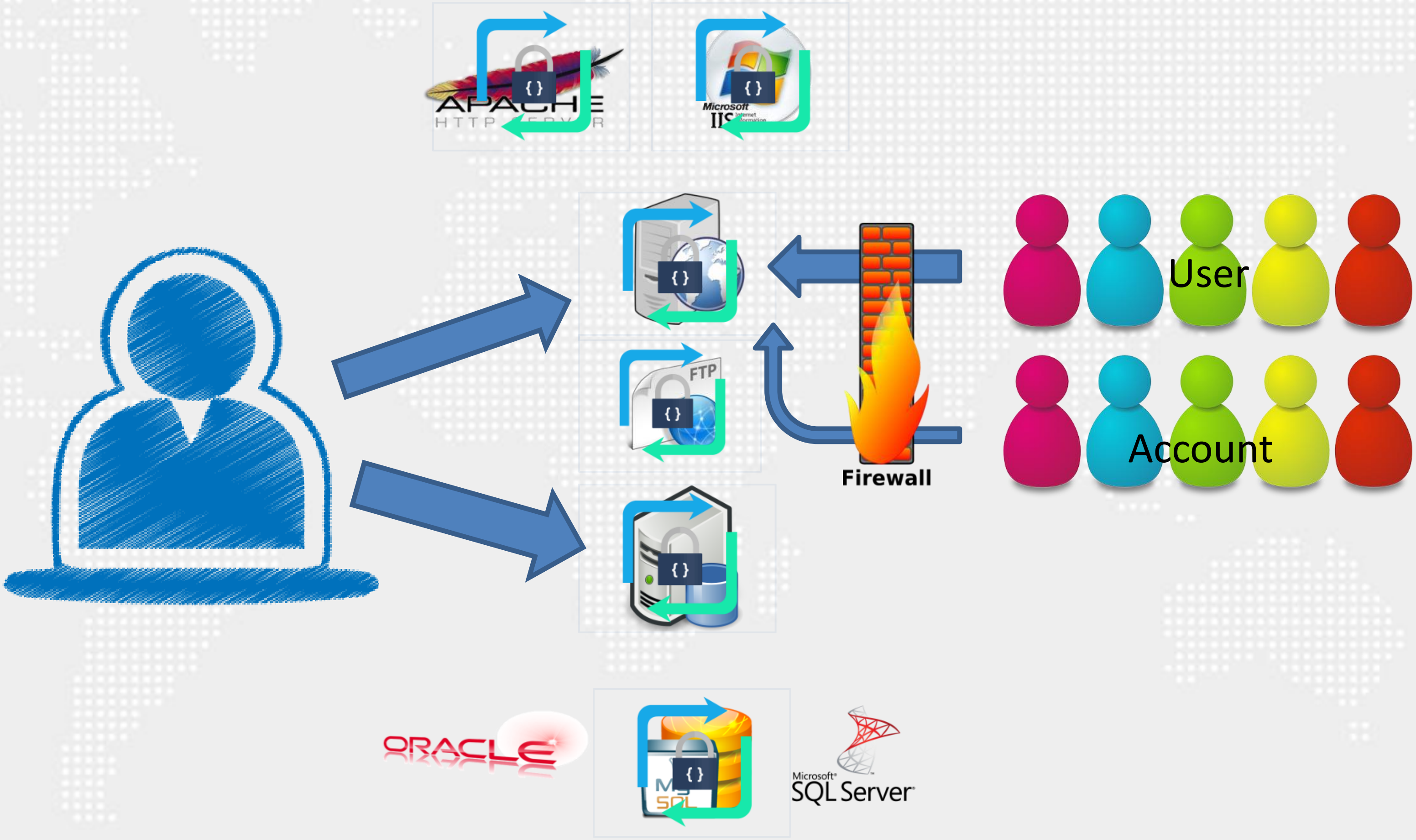
Trust this certificate and carry on connecting?

☐ Always trust certificate in future sessions.

MS Windows Server 2012



MS Windows Server 2012



MS Windows Server 2012

Vulnerability Assessment Software

Nessus®

OpenVAS
Open Vulnerability Assessment System

RETINA
NETWORK SCANNER

Microsoft Baseline Security Analyzer

nexpose®

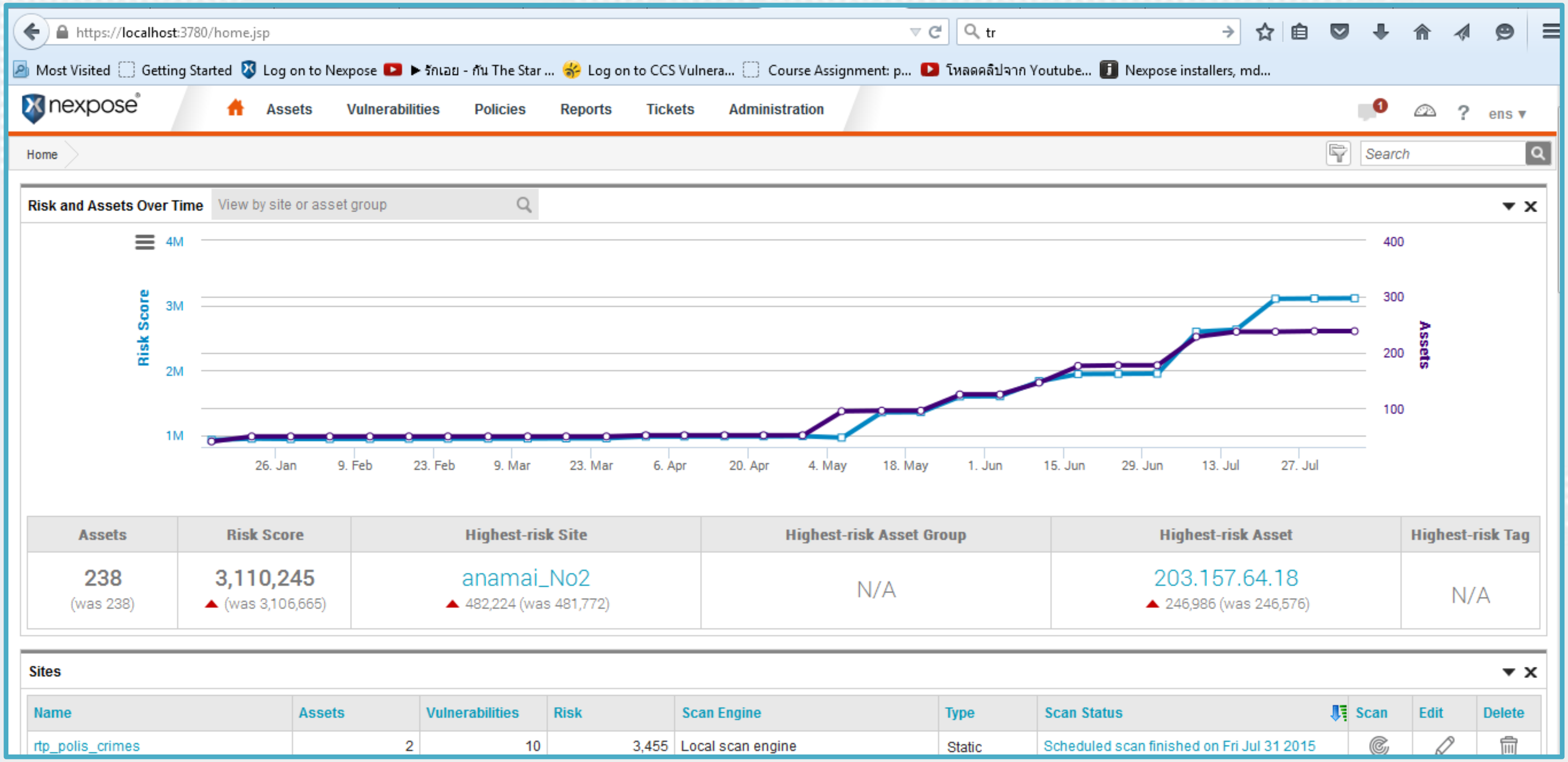
GFI LanGuard™
Network security scanner and patch management

MS Windows Server 2012

Rapid7 Nexpose

EGA e-Government Agency THAILAND

nexpose®



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
238 (was 238)	3,110,245 ▲ (was 3,106,665)	anamai_No2 ▲ 482,224 (was 481,772)	N/A	203.157.64.18 ▲ 246,986 (was 246,576)	N/A

Sites

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
rtp_polis_crimes	2	10	3,455	Local scan engine	Static	Scheduled scan finished on Fri Jul 31 2015			

MS Windows Server 2012

Rapid7 Nexpose

Nexpose: System Requirements
Officially Supported Systems
Minimum Hardware
2 GHz+ processor (Dual-core processor recommended)
8 GB RAM (16 GB recommended)
80 GB+ available disk space (10 GB for Community Edition)
10 GB+ available disk space for Scan engines
English operating system with English/United States regional settings
100 Mbps network interface card (1 Gbps NIC recommended)

Browsers
Google Chrome (latest) (RECOMMENDED)
Mozilla Firefox (latest)
Mozilla Firefox ESR (latest)
Microsoft Internet Explorer 9*, 10, 11

MS Windows Server 2012

Rapid7 Nexpose

Operating Systems

64-bit versions of the following platforms are supported.

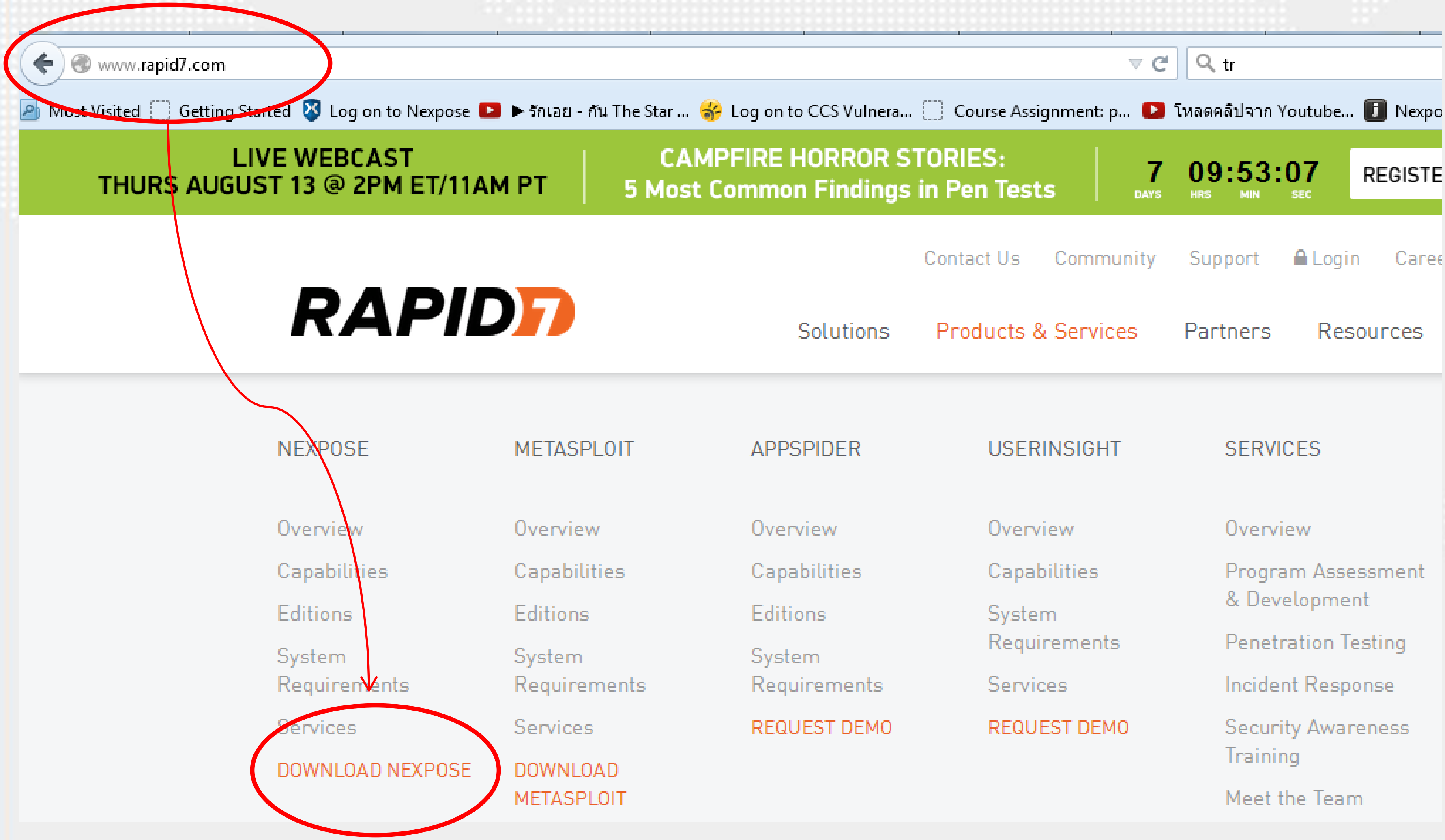
Ubuntu Linux 12.04 LTS (RECOMMENDED)
Ubuntu Linux 14.04 LTS
Ubuntu Linux 10.04 LTS*
Microsoft Windows Server 2008 R2
Microsoft Windows Server 2012 R2
Microsoft Windows 8.1
Microsoft Windows 7 SP1+
Red Hat Enterprise Linux Server 6.5 or later
Red Hat Enterprise Linux Server 5.10 or later
Kali Linux 1.0.x
Virtual Machines on VMware ESXi 5.x, VMware vCenter Server 5.x

MS Windows Server 2012

Rapid7 Nexpose

EGA e-Government Agency THAILAND

nexpose®



www.rapid7.com

Most Visited | Getting Started | Log on to Nexpose | ▶ รักเลย - กัน The Star ... | Log on to CCS Vulnera... | Course Assignment: p... | โหลดคลิปจาก Youtube... | Nexpo

LIVE WEBCAST
THURS AUGUST 13 @ 2PM ET/11AM PT

CAMPFIRE HORROR STORIES:
5 Most Common Findings in Pen Tests

7 DAYS 09:53:07 HRS MIN SEC

REGISTE

Contact Us | Community | Support | Login | Caree

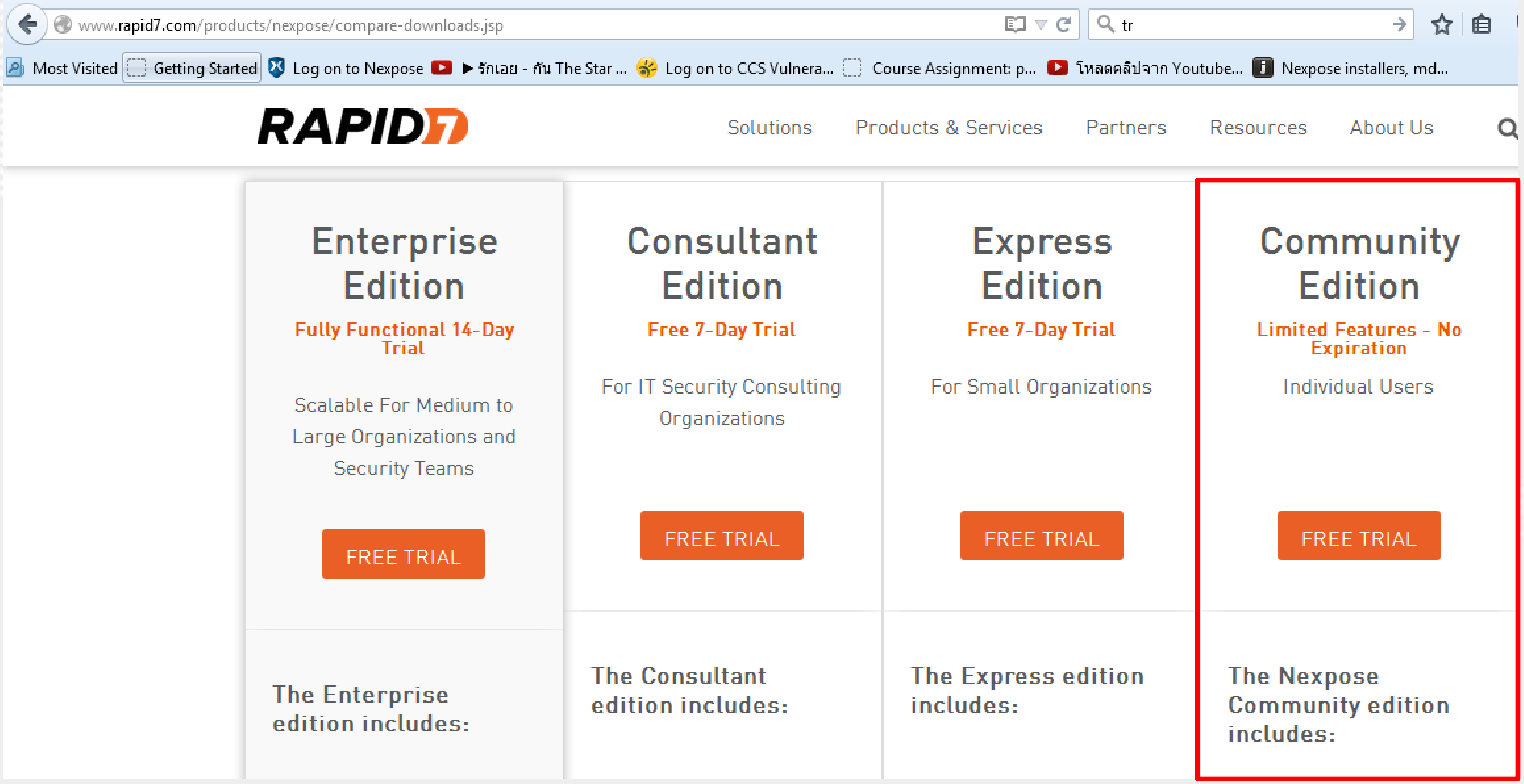
RAPID7

Solutions | Products & Services | Partners | Resources

NEXPOSE	METASPLOIT	APPSPIDER	USERINSIGHT	SERVICES
Overview	Overview	Overview	Overview	Overview
Capabilities	Capabilities	Capabilities	Capabilities	Program Assessment & Development
Editions	Editions	Editions	System Requirements	Penetration Testing
System Requirements	System Requirements	System Requirements	Services	Incident Response
Services	Services	REQUEST DEMO	REQUEST DEMO	Security Awareness Training
DOWNLOAD NEXPOSE	DOWNLOAD METASPLOIT			Meet the Team

MS Windows Server 2012

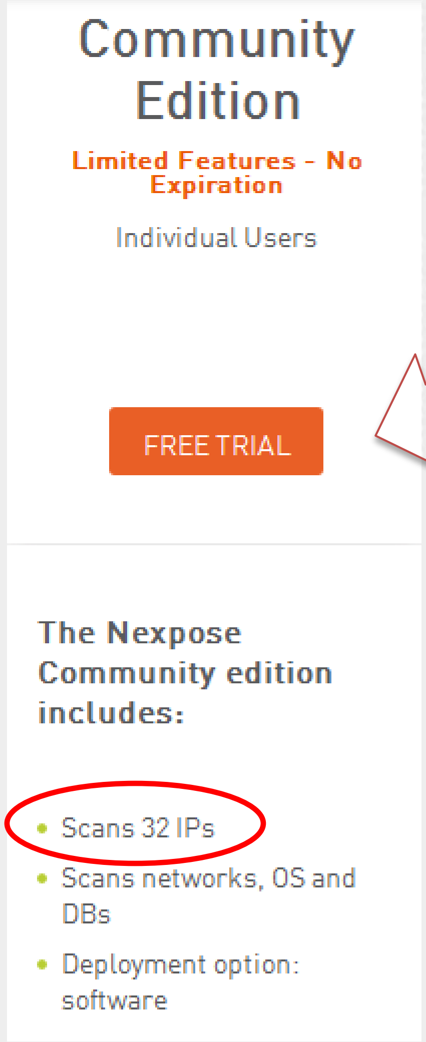
Rapid7 Nexpose



Enterprise Edition	Consultant Edition	Express Edition	Community Edition
Fully Functional 14-Day Trial	Free 7-Day Trial	Free 7-Day Trial	Limited Features - No Expiration
Scalable For Medium to Large Organizations and Security Teams	For IT Security Consulting Organizations	For Small Organizations	Individual Users
FREE TRIAL	FREE TRIAL	FREE TRIAL	FREE TRIAL
The Enterprise edition includes:	The Consultant edition includes:	The Express edition includes:	The Nexpose Community edition includes:

MS Windows Server 2012

Rapid7 Nexpose



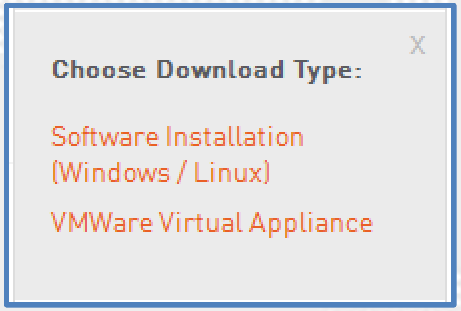
Community Edition

Limited Features - No Expiration

Individual Users

The Nexpose Community edition includes:

- Scans 32 IPs
- Scans networks, OS and DBs
- Deployment option: software



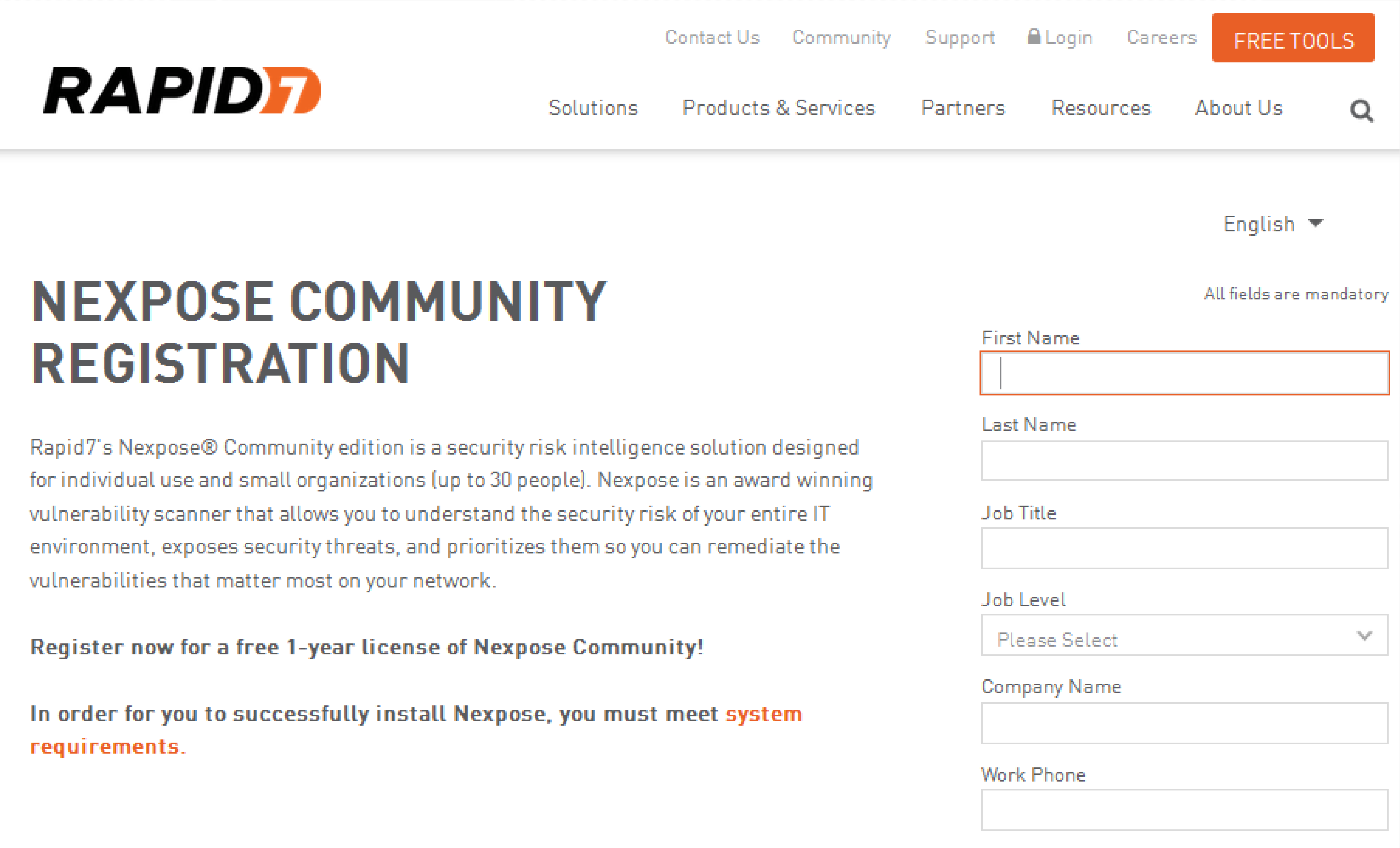
Choose Download Type:

Software Installation (Windows / Linux)

VMWare Virtual Appliance

MS Windows Server 2012

Rapid7 Nexpose



NEXPOSE COMMUNITY REGISTRATION

Rapid7's Nexpose® Community edition is a security risk intelligence solution designed for individual use and small organizations (up to 30 people). Nexpose is an award winning vulnerability scanner that allows you to understand the security risk of your entire IT environment, exposes security threats, and prioritizes them so you can remediate the vulnerabilities that matter most on your network.

Register now for a free 1-year license of Nexpose Community!

In order for you to successfully install Nexpose, you must meet system requirements.

All fields are mandatory

First Name

Last Name

Job Title

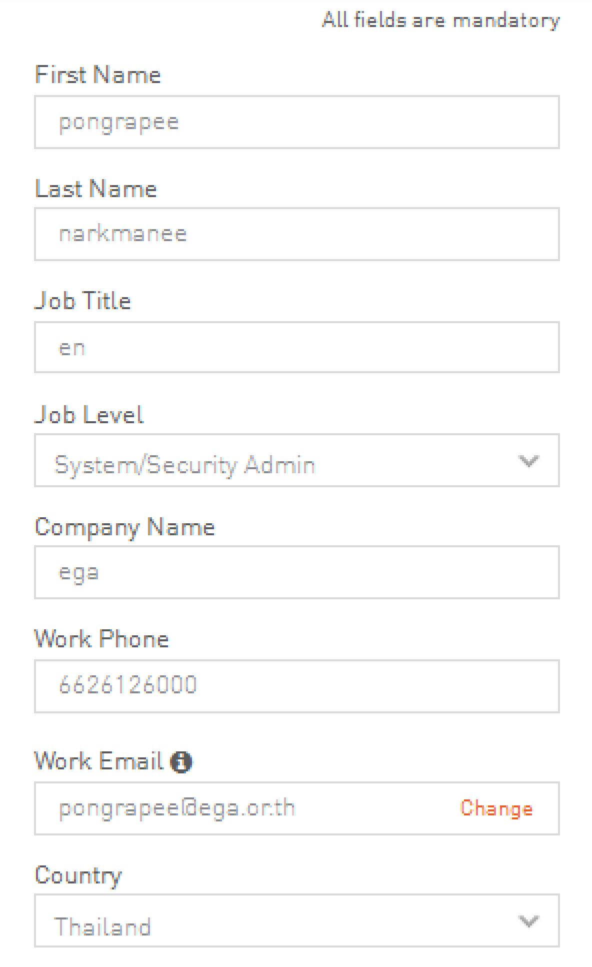
Job Level
Please Select

Company Name

Work Phone

MS Windows Server 2012

Rapid7 Nexpose



All fields are mandatory

First Name: pongrapee

Last Name: narkmanee

Job Title: en

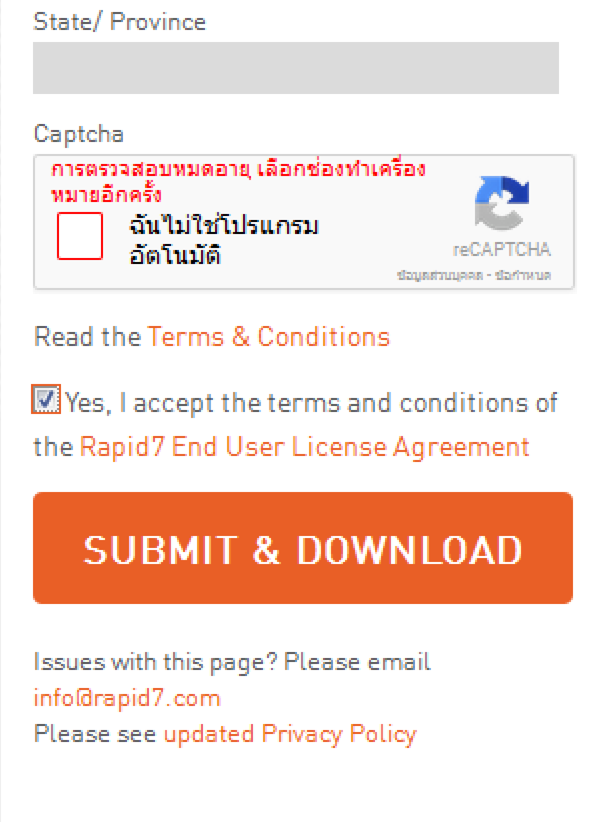
Job Level: System/Security Admin

Company Name: ega

Work Phone: 6626126000

Work Email: pongrapee@ega.or.th Change

Country: Thailand



State/ Province

Captcha

การตรวจสอบหมดอายุ เลือกช่องทำเครื่องหมายอีกครั้ง

□ ฉันไม่ใช่โปรแกรมอัตโนมัติ

Read the Terms & Conditions

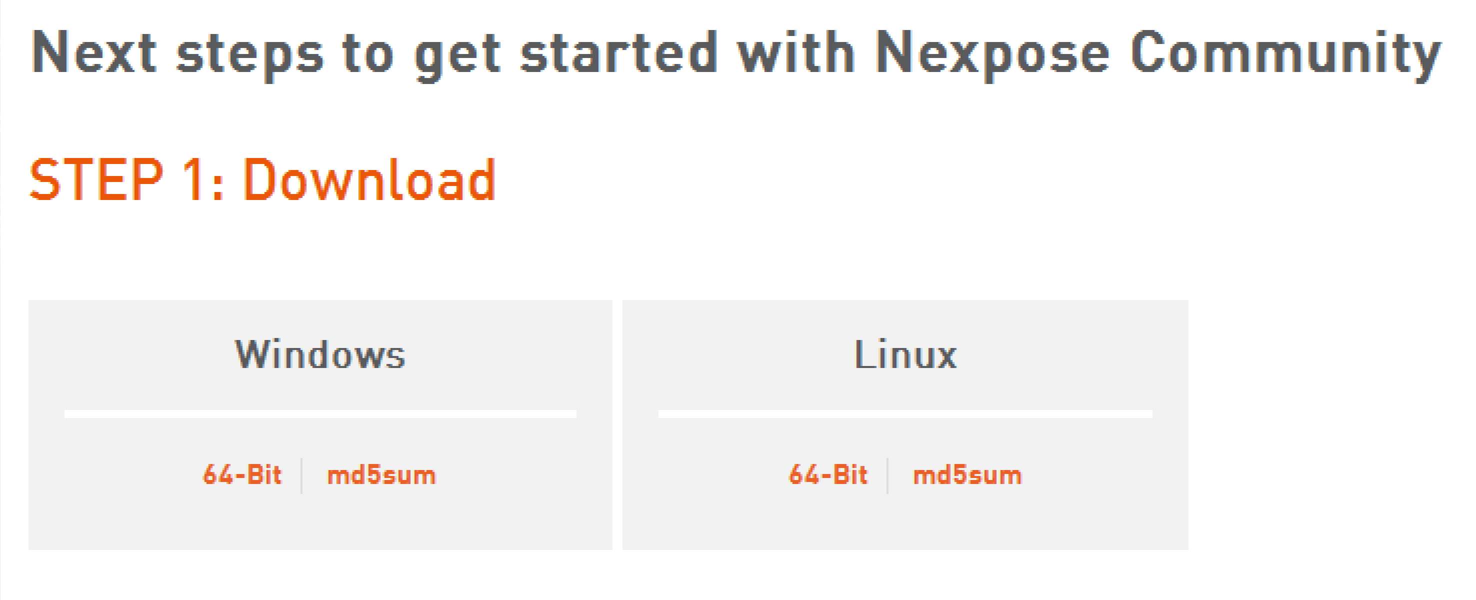
☑ Yes, I accept the terms and conditions of the Rapid7 End User License Agreement

Issues with this page? Please email info@rapid7.com

Please see updated Privacy Policy

MS Windows Server 2012

Rapid7 Nexpose



Next steps to get started with Nexpose Community

STEP 1: Download

Windows

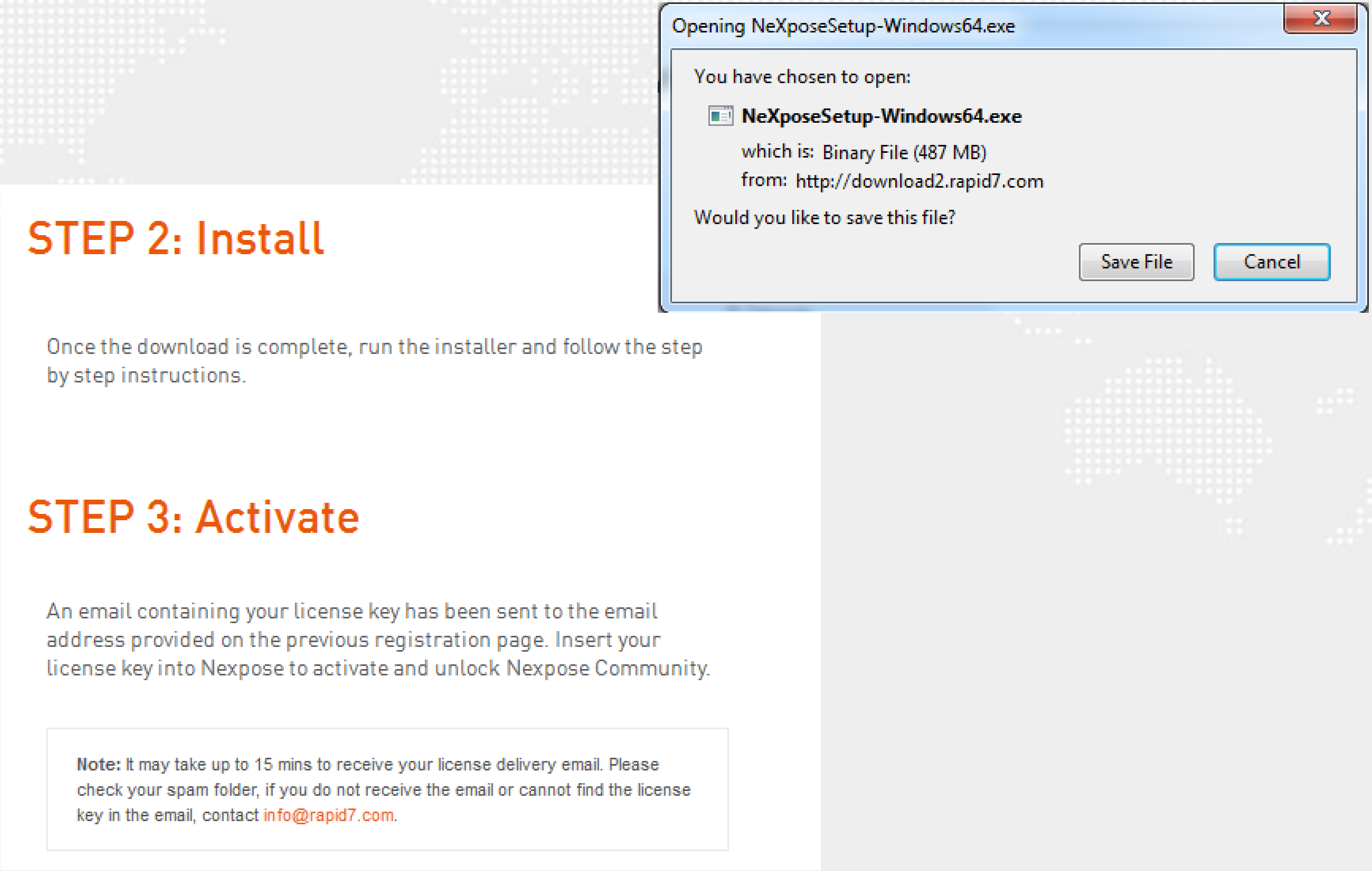
64-Bit | md5sum

Linux

64-Bit | md5sum

MS Windows Server 2012

Rapid7 Nexpose



Opening NeXposeSetup-Windows64.exe

You have chosen to open:

NeXposeSetup-Windows64.exe

which is: Binary File (487 MB)

from: http://download2.rapid7.com

Would you like to save this file?

STEP 2: Install

Once the download is complete, run the installer and follow the step by step instructions.

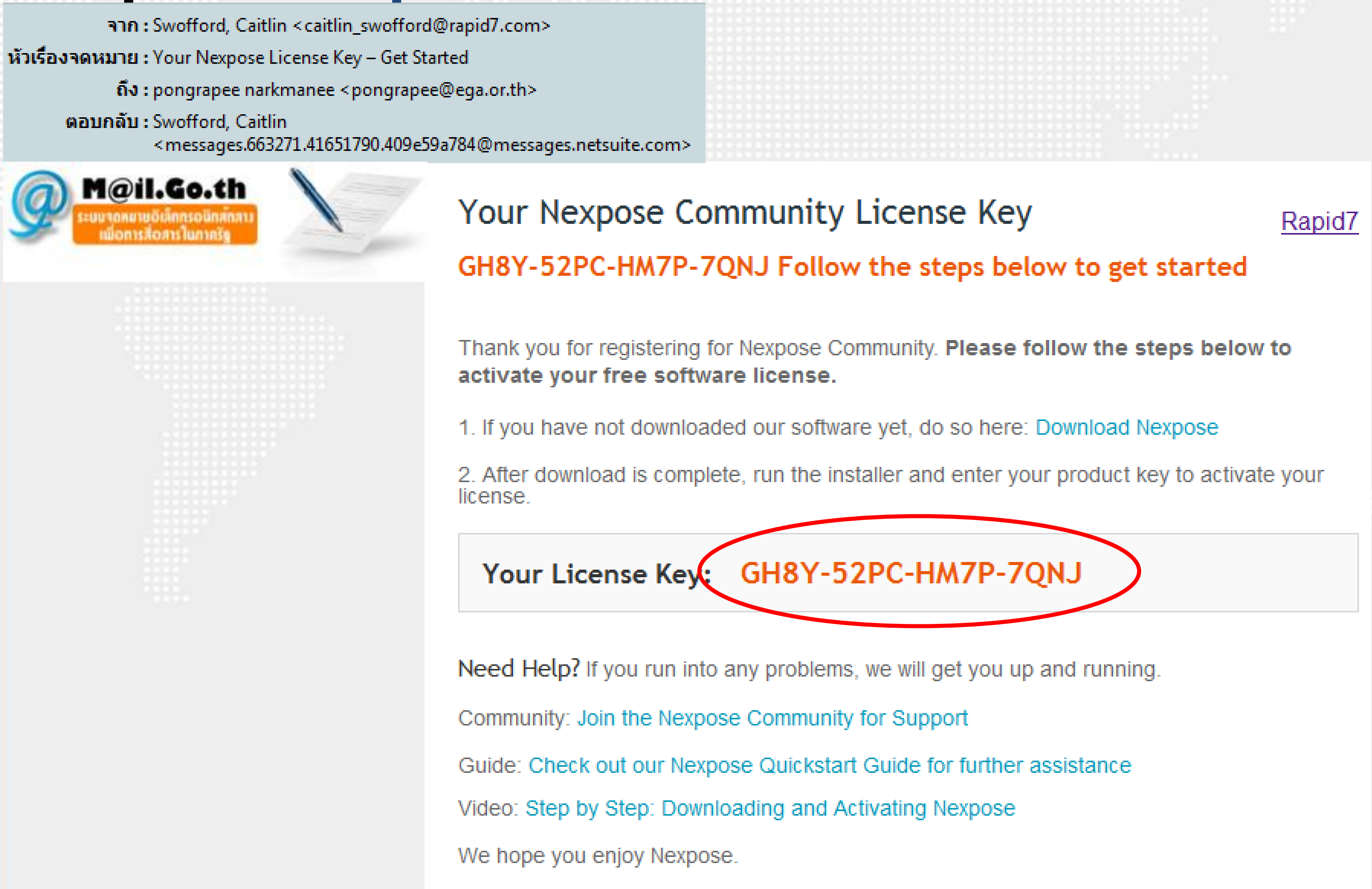
STEP 3: Activate

An email containing your license key has been sent to the email address provided on the previous registration page. Insert your license key into Nexpose to activate and unlock Nexpose Community.

Note: It may take up to 15 mins to receive your license delivery email. Please check your spam folder, if you do not receive the email or cannot find the license key in the email, contact info@rapid7.com.

MS Windows Server 2012

Rapid7 Nexpose



จาก : Swofford, Caitlin <caitlin_swofford@rapid7.com>
หัวเรื่องจดหมาย : Your Nexpose License Key – Get Started
ถึง : pongrapee narkmanee <pongrapee@ega.or.th>
ตอบกลับ : Swofford, Caitlin <messages.663271.41651790.409e59a784@messages.netsuite.com>

Your Nexpose Community License Key

GH8Y-52PC-HM7P-7QNJ Follow the steps below to get started

Thank you for registering for Nexpose Community. **Please follow the steps below to activate your free software license.**

1. If you have not downloaded our software yet, do so here: Download Nexpose

2. After download is complete, run the installer and enter your product key to activate your license.

Your License Key: GH8Y-52PC-HM7P-7QNJ

Need Help? If you run into any problems, we will get you up and running.

Community: Join the Nexpose Community for Support

Guide: Check out our Nexpose Quickstart Guide for further assistance

Video: Step by Step: Downloading and Activating Nexpose

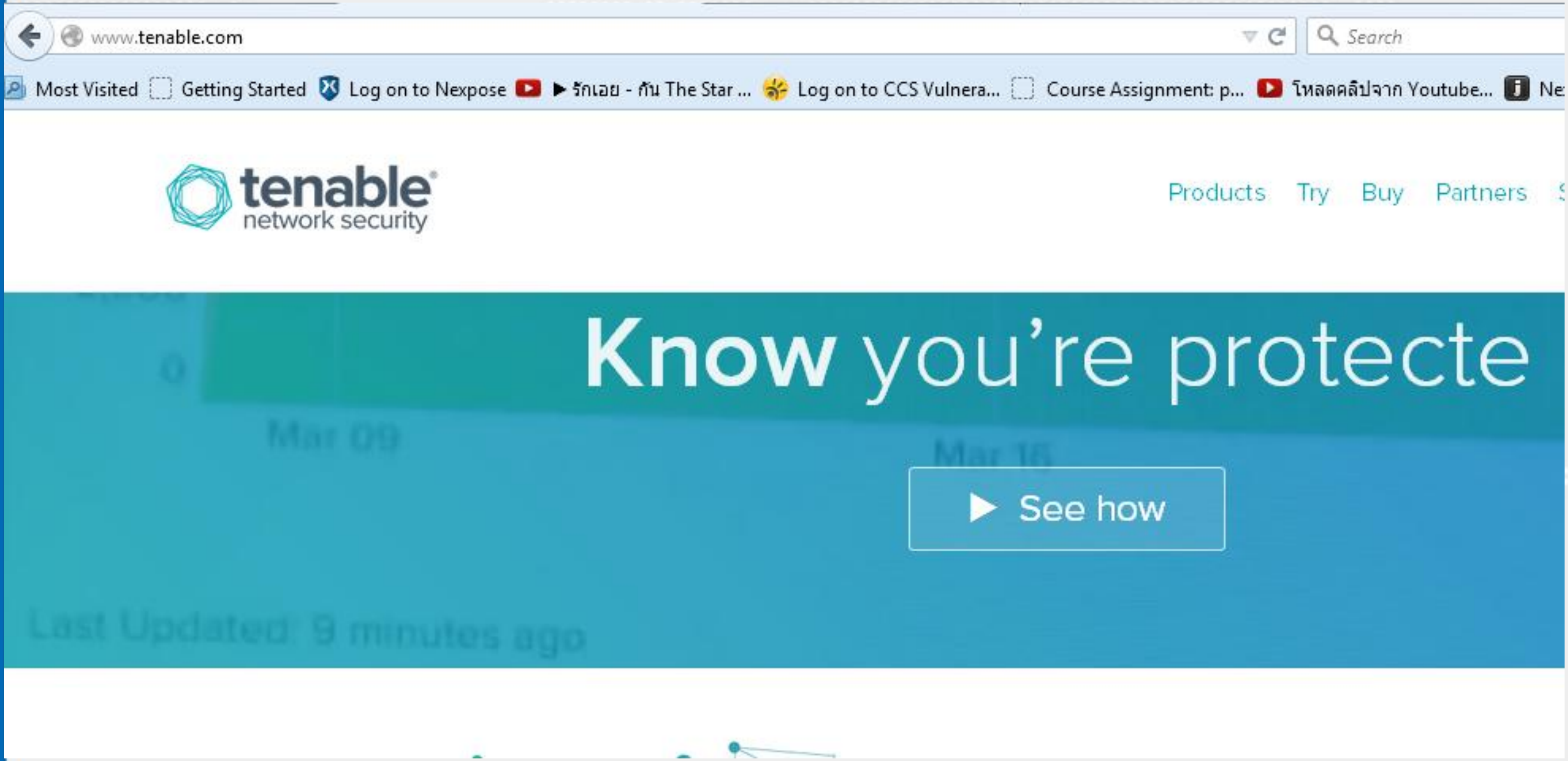
We hope you enjoy Nexpose.

MS Windows Server 2012

Rapid7 Nexpose

ทดสอบ Scan ช่องโหว่

MS Windows Server 2012


www.tenable.com

Search

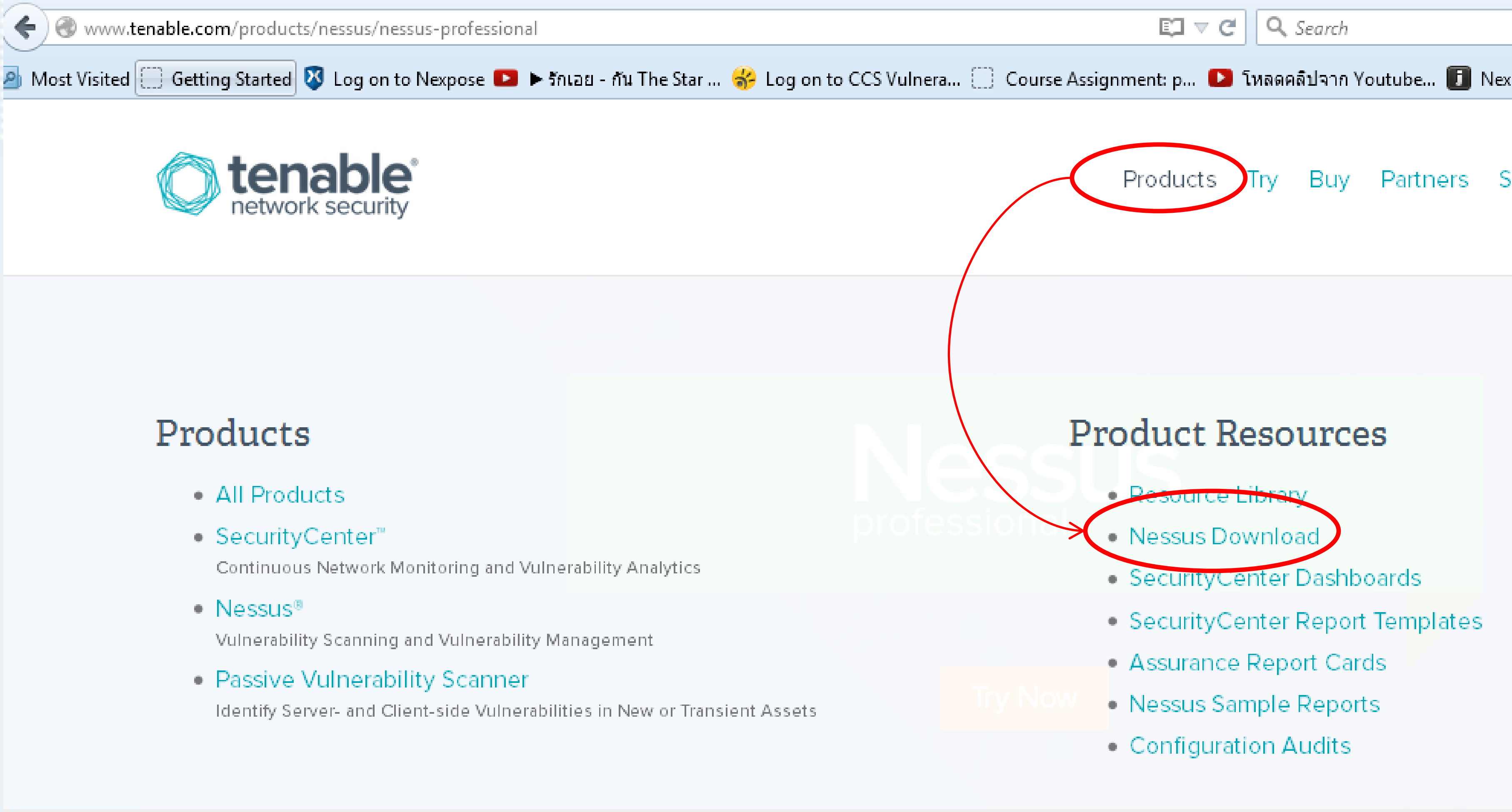
Most Visited · Getting Started · Log on to Nexpose · ▶ รักเลย - กัน The Star ... · Log on to CCS Vulnera... · Course Assignment: p... · โหลดคลิปจาก Youtube... · Ne

MS Windows Server 2012

tenable® network security

EGA e-Government Agency THAILAND

Nessus



www.tenable.com/products/nessus/nessus-professional

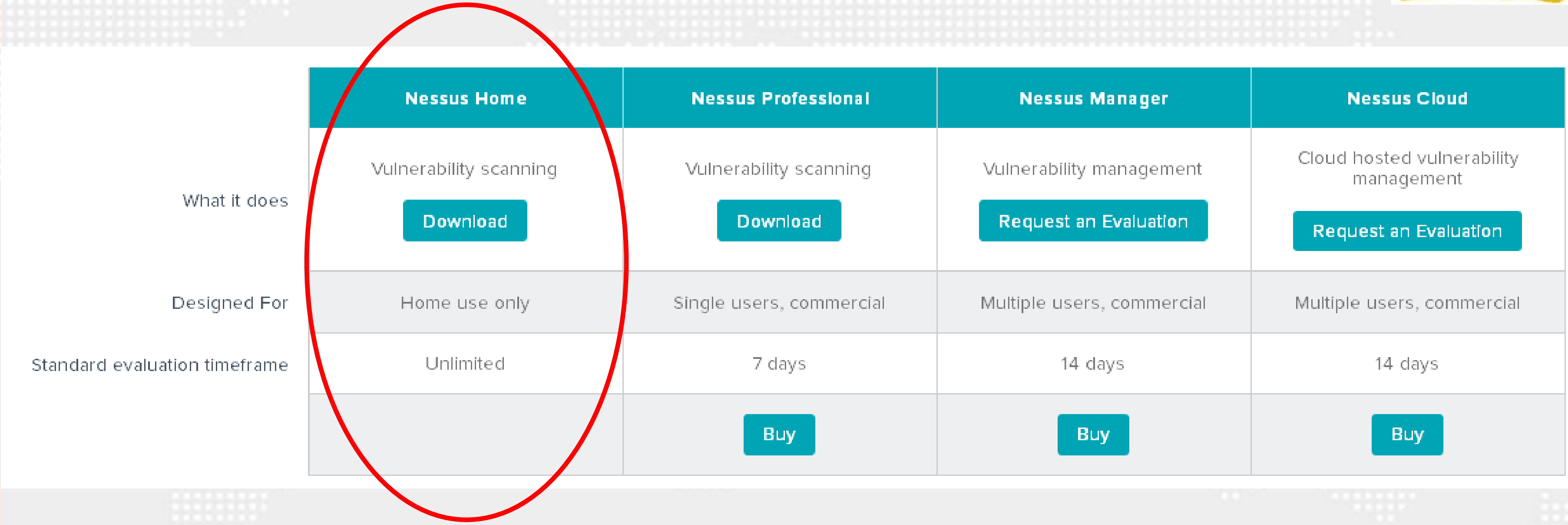
Products

- All Products
- SecurityCenter™
  Continuous Network Monitoring and Vulnerability Analytics
- Nessus®
  Vulnerability Scanning and Vulnerability Management
- Passive Vulnerability Scanner
  Identify Server- and Client-side Vulnerabilities in New or Transient Assets

Product Resources

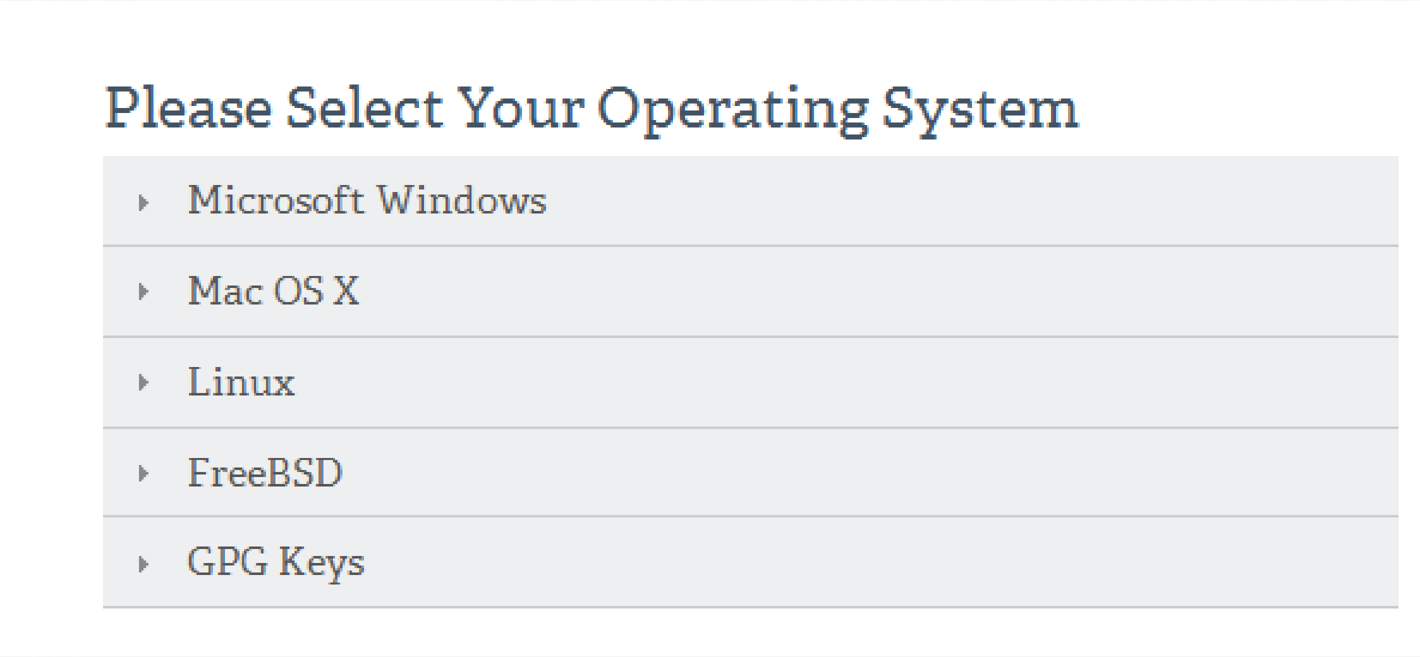
- Resource Library
- Nessus Download
- SecurityCenter Dashboards
- SecurityCenter Report Templates
- Assurance Report Cards
- Nessus Sample Reports
- Configuration Audits

MS Windows Server 2012



	Nessus Home	Nessus Professional	Nessus Manager	Nessus Cloud
What it does	Vulnerability scanning Download	Vulnerability scanning Download	Vulnerability management Request an Evaluation	Cloud hosted vulnerability management Request an Evaluation
Designed For	Home use only	Single users, commercial	Multiple users, commercial	Multiple users, commercial
Standard evaluation timeframe	Unlimited	7 days	14 days	14 days
		Buy	Buy	Buy

MS Windows Server 2012



Please Select Your Operating System

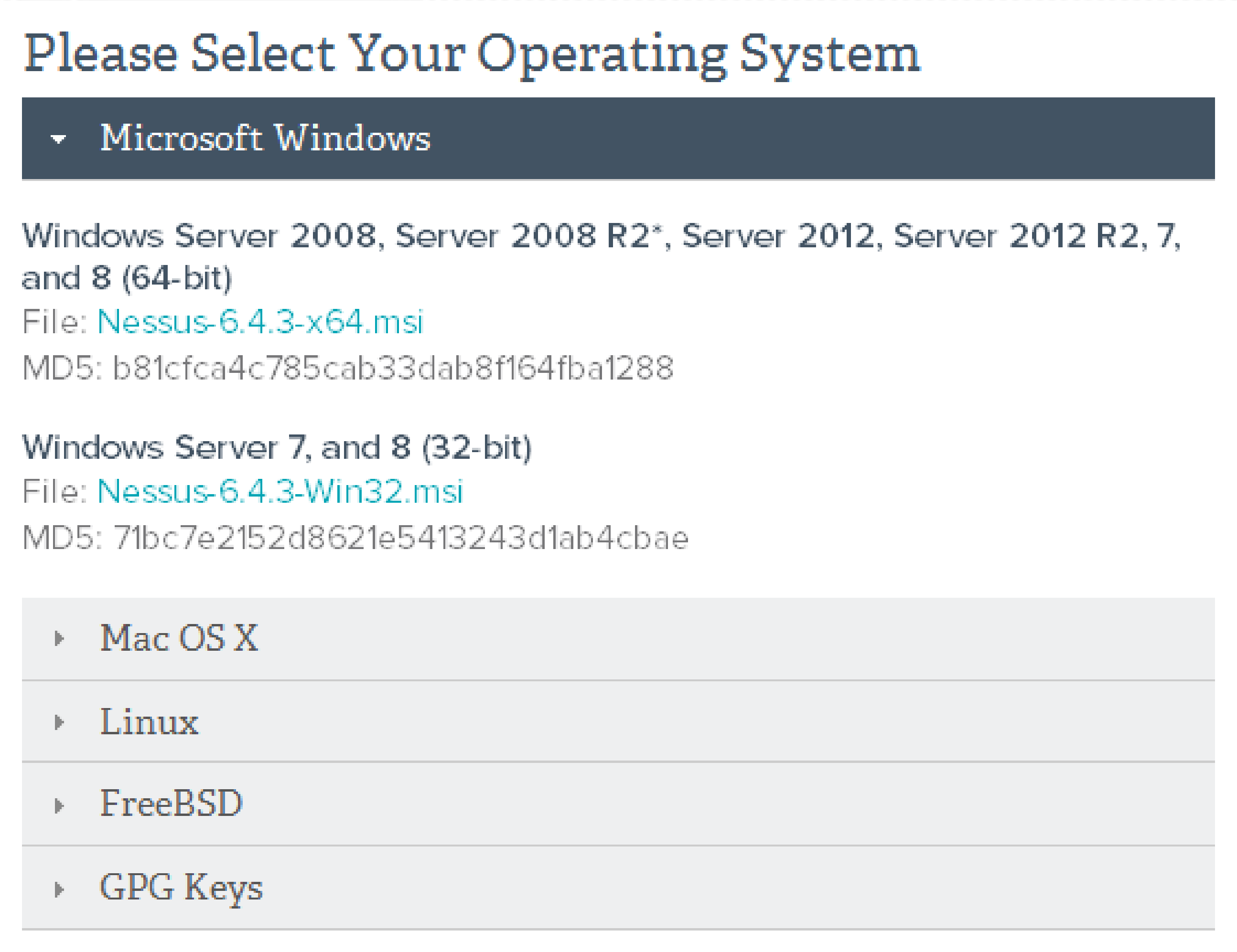
- Microsoft Windows
- Mac OS X
- Linux
- FreeBSD
- GPG Keys

MS Windows Server 2012

tenable
network security

EGA
e-Government Agency
THAILAND

Nessus



Please Select Your Operating System

▾ Microsoft Windows

Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, and 8 (64-bit)
File: Nessus-6.4.3-x64.msi
MD5: b81cfca4c785cab33dab8f164fba1288

Windows Server 7, and 8 (32-bit)
File: Nessus-6.4.3-Win32.msi
MD5: 71bc7e2152d8621e5413243d1ab4cbae

▸ Mac OS X

▸ Linux

▸ FreeBSD

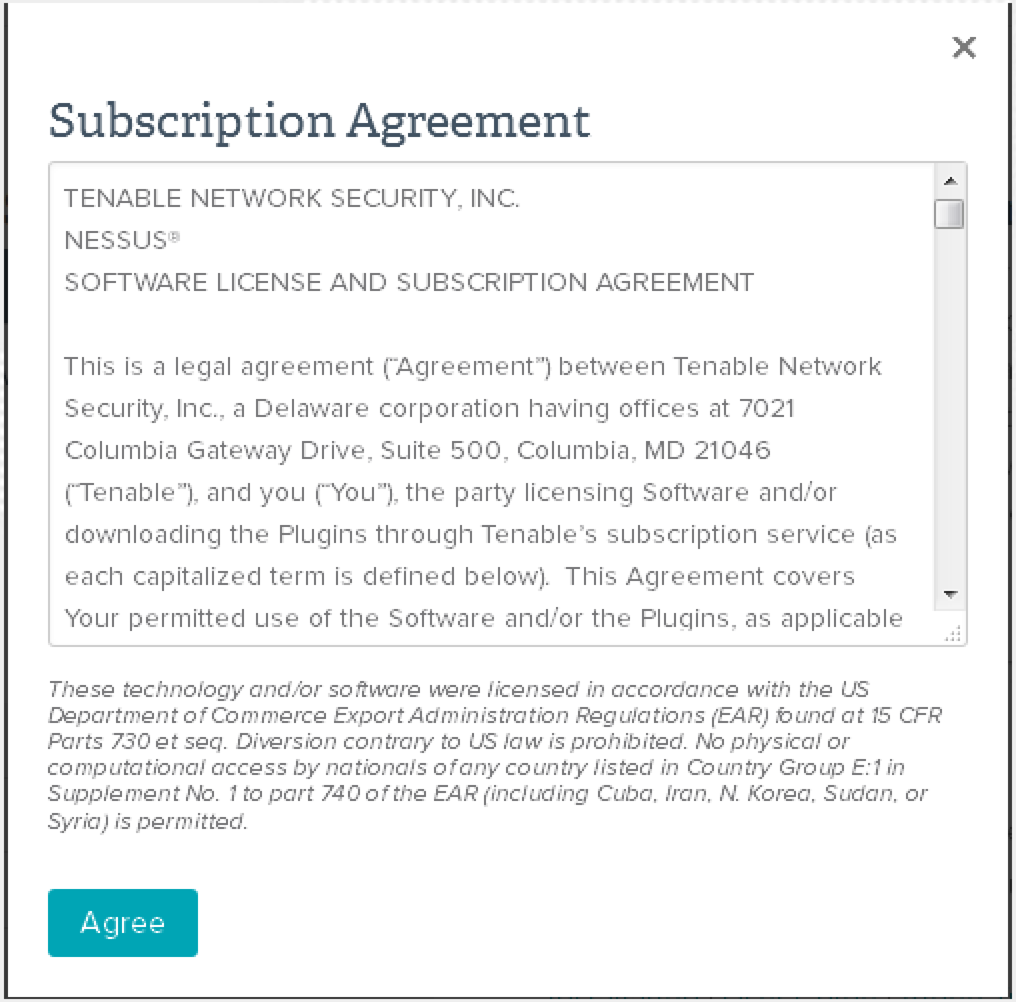
▸ GPG Keys

MS Windows Server 2012

tenable network security

EGA e-Government Agency THAILAND

Nessus



Subscription Agreement

TENABLE NETWORK SECURITY, INC.

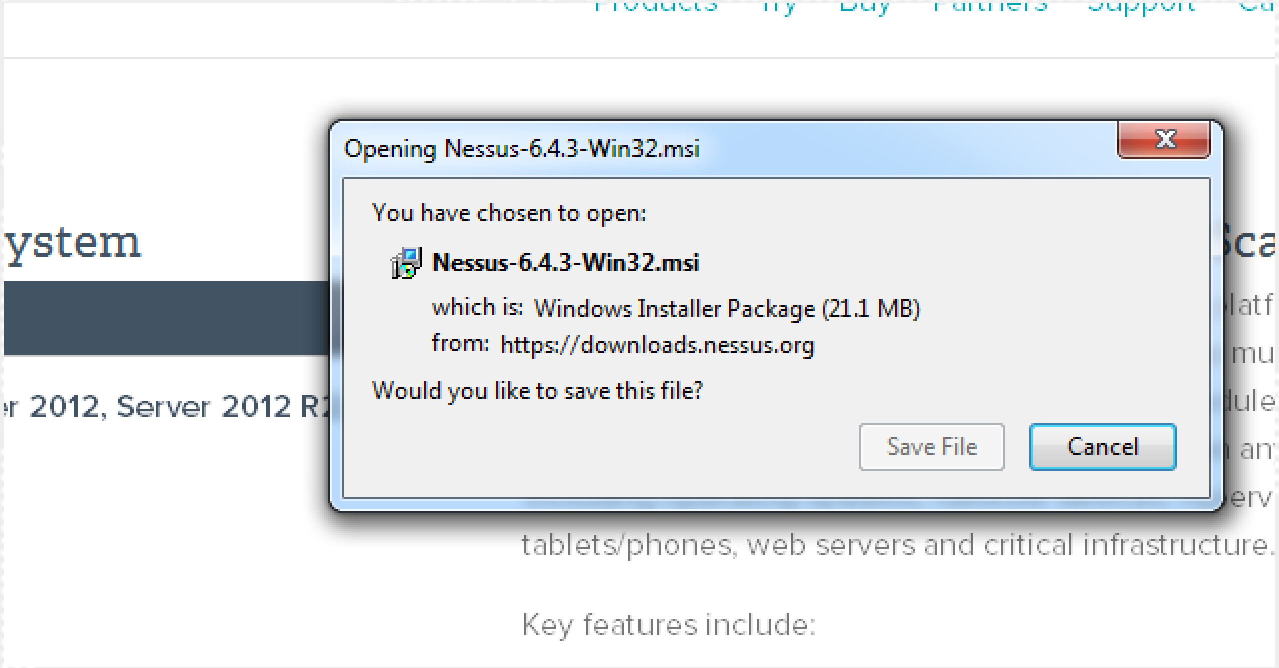
NESSUS®

SOFTWARE LICENSE AND SUBSCRIPTION AGREEMENT

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you ("You"), the party licensing Software and/or downloading the Plugins through Tenable's subscription service (as each capitalized term is defined below). This Agreement covers Your permitted use of the Software and/or the Plugins, as applicable

These technology and/or software were licensed in accordance with the US Department of Commerce Export Administration Regulations (EAR) found at 15 CFR Parts 730 et seq. Diversion contrary to US law is prohibited. No physical or computational access by nationals of any country listed in Country Group E:1 in Supplement No. 1 to part 740 of the EAR (including Cuba, Iran, N. Korea, Sudan, or Syria) is permitted.

MS Windows Server 2012



Opening Nessus-6.4.3-Win32.msi

You have chosen to open:

Nessus-6.4.3-Win32.msi

which is: Windows Installer Package (21.1 MB)
from: https://downloads.nessus.org

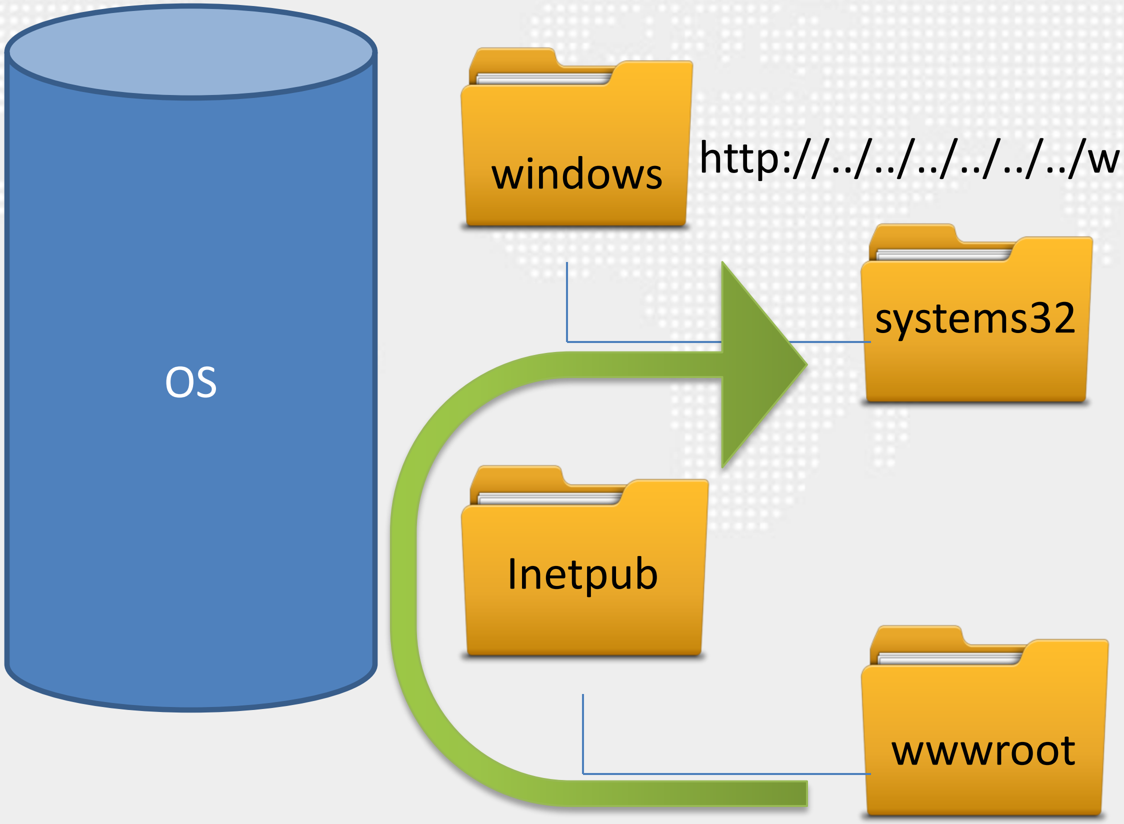
Would you like to save this file?

MS Windows Server 2012

Tip Directory traversal

MS Windows Server 2012

Web Server

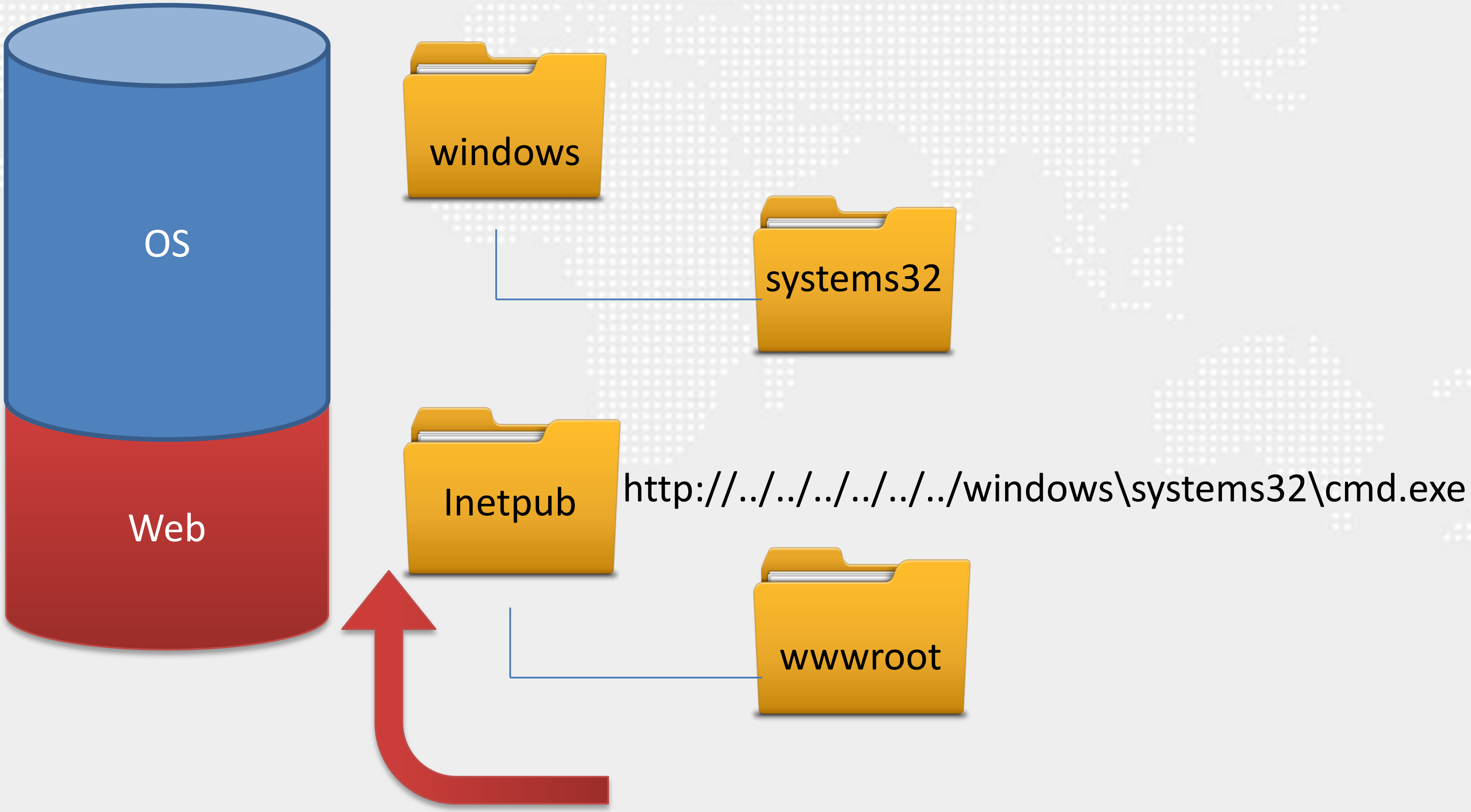


http://../../../../../../windows\systems32\cmd.exe

http://../../../../../../windows\systems32\cmd.exe

MS Windows Server 2012

Web Server



https://pentestlab.wordpress.com/2012/06/29/directory-traversal-cheat-sheet/

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